Claim Chart – USP 8,051,181 relative to Mattaway

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
1.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising	*See, e.g.*, *Mattaway* at 3:8-20, 11:13-15, 17:44-48, 26:43-55, 26:63-67, 40:27, Figure 1	Request at §V.B(1)
1(a).	receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device;	*See, e.g.*, *Mattaway* at 8:25-44, 18:41-45, Figure 16A	Request at §V.B(1)
1(b).	sending a message over a secure communication link from the first device to the second device.	*See, e.g.*, *Mattaway* at 7:33-37, 25:32-34	Request at §V.B(1)
2.	[a] method of using a first device to communicate with a second device having a secure name, the method comprising:	*See, e.g.*, *Mattaway* at 3:8-20, Figure 1	Request at §V.B(2)
2(a).	from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;	*See, e.g.*, *Mattaway* at 7:24-37, 17:44-48, 40:27	Request at §V.B(2)
2(b).	at the first device, receiving a message containing the network address associated with the secure name of the second device;	*See, e.g.*, *Mattaway* at 7:32-37	Request at §V.B(2)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
2(c).	from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.	*See, e.g.*, *Mattaway* at 7:33-37, 25:32-34	Request at §V.B(2)
3.	The method according to claim 2, wherein the secure name of the second device is a secure domain name.	*See, e.g.*, *Beser* at 10:38-41	Request at §V.C(3)(a)
4.	The method according to claim 2, wherein the secure name indicates security.	*See, e.g.*, *Mattaway* at 25:32-34 *See, e.g.*, *Beser* at 11:13-25	Request at §V.C(3)(b)
5.	The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.	*See, e.g.*, *Mattaway* at 25:32-34	Request at §V.B(3)
6.	The method according to claim 5, further including decrypting the message.	*See, e.g.*, *Mattaway* at 25:32-34	Request at §V.B(4)
7.	The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.	*See, e.g.*, *Mattaway* at 6:37-45, 17:1-5	Request at §V.B(5)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
8.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device	*See, e.g.*, *Mattaway* at 7:32-37	Request at §V.B(6)
9.	The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.	*See, e.g.*, *Mattaway* at 25:32-34	Request at §V.B(7)
10.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.	*See, e.g.*, *Mattaway* at 25:32-34 *See, e.g.*, *RFC2401* at 4-5, 24-26	Request at §V.C(3)(c) and §V.C(4)(a)
11.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.	*See, e.g.*, *Mattaway* at 25:32-34 *See, e.g.*, *Beser* at 2:6-12, 6:58-59, 12:6-19 *See, e.g.*, *RFC2401* at 4-5, 24-26	Request at §V.C(3)(d) and §V.C(4)(b)
12.	The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols	*See, e.g.*, *Mattaway* at 6:37-45, 17:1-5	Request at §V.B(8)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
13.	The method according to claim 2, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.	*See, e.g., Mattaway* at 3:8-20, Figure 1	Request at §V.B(9)
14.	The method according to claim 2, further including supporting a plurality of services over the secure communication link.	*See, e.g., Mattaway* at 4:38-41, 5:50-54, 6:37-45, 17:1-5	Request at §V.B(10)
15.	The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.	*See, e.g., Mattaway* at 4:38-41, 5:50-54, 6:37-45, 17:1-5	Request at §V.B(11)
16.	The method of claim 15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.	*See, e.g., Mattaway* at 4:38-41, 17:5-9	Request at §V.B(12)
17.	The method of claim 15, wherein the plurality of services comprises audio, video or a combination thereof.	*See, e.g., Mattaway* at 4:38-41, 17:5-9	Request at §V.B(13)
18.	The method according to claim 2, wherein the secure communication link is an authenticated link.	*See, e.g., Mattaway* at 25:32-34 *See, e.g., Beser* at 11:22-25	Request at §V.C(3)(e)

Claim Chart – USP 8,051,181 relative to Mattaway

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
19.	The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.	*See, e.g.*, *Mattaway* at 4:22-24, 4:37-42	Request at §V.B(14)
20.	The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.	*See, e.g.*, *Mattaway* at 4:22-29, 4:37-42	Request at §V.B(15)
21.	The method according to claim 2, further including providing an unsecured name associated with the device.	*See, e.g.*, *Mattaway* at 11:13-15, 26:43-55, 26:63-67	Request at §V.B(16)
22.	The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.	*See, e.g.*, *Mattaway* at 3:8-20, Figure 1	Request at §V.B(17)
23.	The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.	*See, e.g.*, *Beser* at 10:38-41	Request at §V.C(3)(f)
24.	A method of using a first device to securely communicate with a second device over a communication network, the method comprising:	*See, e.g.*, *Mattaway* at 3:8-20, Figure 1	Request at §V.B(18)
24(a).	at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address	*See, e.g.*, *Mattaway* at 6:60-65	Request at §V.B(18)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
24(b).	receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device.	*See, e.g.*, *Mattaway* at 7:32-37, 8:25-44, 18:41-45, Figure 16A	Request at §V.B(18)
24(c).	sending a message securely from the first device to the second device.	*See, e.g.*, *Mattaway* at 25:32-34	Request at §V.B(18)
25.	The method according to claim 24, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.	*See, e.g.*, *Mattaway* at 6:60-65, 25:32-34	Request at §V.B(19)
26.	A method of using a first device to communicate with a second device over a communication network, the method comprising:	*See, e.g.*, *Mattaway* at 3:8-20, Figure 1	Request at §V.B(20)
26(a).	from the first device requesting and obtaining registration of an unsecured name associated with the first device	*See, e.g.*, *Mattaway* at 11:13-15, 26:43-55, 26:63-67	Request at §V.B(20)
26(b).	from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device.	*See, e.g.*, *Mattaway* at 6:60-65	Request at §V.B(20)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
26(c).	receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device	*See, e.g.*, *Mattaway* at 7:32-37, 8:25-44, 18:41-45, Figure 16A	Request at §V.B(20)
26(d).	from the first device sending a message securely from the first device to the second device	*See, e.g.*, *Mattaway* at 25:32-34	Request at §V.B(20)
27(a).	The method of claim 26, wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device	*See, e.g.*, *Mattaway* at 11:13-15, 26:43-55, 26:63-67	Request at §V.B(21)
27(b).	wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.	*See, e.g.*, *Mattaway* at 6:60-65	Request at §V.B(21)
28.	A, non-transitory machine-readable medium comprising instructions for:	*See, e.g.*, *Mattaway* at 3:8-20, Figure 1	Request at §V.B(22)
28(a)	sending a message to a secure name service, the message requesting a network address associated with a secure name of a device	*See, e.g.*, *Mattaway* at 7:24-37	Request at §V.B(22)
28(b).	receiving a message containing the network address associated with the secure name of the device	*See, e.g.*, *Mattaway* at 7:32-37	Request at §V.B(22)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
28(c).	sending a message to the network address associated with the secure name of the device using a secure communication link.	*See, e.g., Mattaway* at 25:32-34	Request at §V.B(22)
29.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:	*See, e.g., Mattaway* at 3:8-20, Figure 1	Request at §V.B(23)
29(a).	receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered	*See, e.g., Mattaway* at 7:32-37, 8:25-44, 18:41-45, Figure 16A	Request at §V.B(23)
29(b).	sending a message securely from the first device to the second device.	*See, e.g., Mattaway* at 25:32-34	Request at §V.B(23)

EXHIBIT B

CERTIFICATE OF SERVICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 8,051,181) Control No.:
)
Filed: February 27, 2007) Group Art Unit: Central Reexamination Unit
)
Issued: November 1, 2011)
) Examiner:
Inventors: Larson et al.)
) Confirmation No.:
For: METHOD FOR ESTABLISHING)
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF)
VIRTUAL PRIVATE NETWORK)

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF SERVICE

I hereby certify that a copy of this correspondence for Petition Under 37 CFR § 1.182 to Permit Consideration of Information in an *Inter Partes* Reexamination Proceeding has been served in its entirety by First Class Mail on the following:

VirnetX Inc.
c/o McDermott Will & Emery
600 13th Street, N.W.
Washington, D.C. 20005-3096

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Reg. No. 43,401
March 28, 2012

EXHIBIT C6

CLAIM CHART - '181 RELATIVE TO JOHNSON

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
1.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising	*See, e.g.*, *Johnson* at Abstract, Figure 1, 1:19-27, 6:25-35, 8:4-9, 9:23-33, 10:36-52; 11:23-24, 12:20-25 *See, e.g.*, *RFC 2131* at 1-3, 6, 8, 9, 26 *See, e.g.*, *RFC 1034* at 11-12	Request at §IX.A(1)
1(a).	receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device;	*See, e.g.*, *Johnson* at 7:10-17, 7:20-27, 8:10-12	Request at §IX.A(1)
1(b).	sending a message over a secure communication link from the first device to the second device.	*See, e.g.*, *Johnson* at 7:20-27, 8:9-18	Request at §IX.A(1)
2.	[a] method of using a first device to communicate with a second device having a secure name, the method comprising:	*See, e.g.*, *Johnson* at Abstract, Figure 1, 1:19-27, 6:25-35, 8:4-9, 9:23-33, 10:36-52, 11:23-24, 12:20-25 *See, e.g.*, *RFC 2131* at 1-3, 6, 8, 9, 26 *See, e.g.*, *RFC 1034* at 11-12	Request at §IX.A(2)
2(a).	from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;	*See, e.g.*, *Johnson* at 11:21-37, Figure 7	Request at §IX.A(2)
2(b).	at the first device, receiving a message containing the network address associated with the secure name of the second device;	*See, e.g.*, *Johnson* at 7:10-17	Request at §IX.A(2)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
2(c).	from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.	*See, e.g., Johnson* at 7:20-27, 8:9-18	Request at §IX.A(2)
3.	The method according to claim 2, wherein the secure name of the second device is a secure domain name.	*See, e.g., Johnson* at 1:19-27 *See, e.g., RFC 1034* at 1, 9, 11-12, 17	Request at §IX.A(3)
4.	The method according to claim 2, wherein the secure name indicates security.	*See, e.g., Johnson* at 1:19-27 *See, e.g., RFC 1034* at 1, 9, 11-12, 17	Request at §IX.A(4)
5.	The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.	*See, e.g., Johnson* at 8:4-8	Request at §IX.A(5)
6.	The method according to claim 5, further including decrypting the message.	*See, e.g., Johnson* at 8:4-8	Request at §IX.A(6)
7.	The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.	*See, e.g., Johnson* at 5:45-47, 7:20-27, 7:49-8:34, 11:21-37, 12:20-25	Request at §IX.A(7)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
8.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device	*See, e.g.*, *Johnson* at 6:25-35, 8:4-9, 9:23-33, 10:36-52, 12:20-25, Figure 1 *See, e.g.*, *RFC 2131* at 1-3	Request at §IX.A(8)
9.	The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.	*See, e.g.*, *Johnson* at 1:29-4:67, 7:20-27 *See, e.g.*, *RFC 2401* at 21, 27	Request at §IX.A(9)
10.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.	*See, e.g.*, *RFC 2401* at 9, 24-25	Request at §IX.A(10)
11.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.	*See, e.g.*, *RFC 2401* at 9, 24-25	Request at §IX.A(11)
12.	The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols	*See, e.g.*, *Johnson* at 1:19-27, Figure 1	Request at §IX.A(12)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
13.	The method according to claim 2, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.	*See, e.g.*, *RFC 2401* at 17	Request at §IX.A(13)
14.	The method according to claim 2, further including supporting a plurality of services over the secure communication link.	*See, e.g.*, *RFC 2401* at 3, 4, 17	Request at §IX.A(14)
15.	The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.	*See, e.g.*, *Johnson* at 10:18-21	Request at §IX.A(15)
16.	The method of claim 15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.	*See, e.g.*, *Johnson* at 10:18-21	Request at §IX.A(16)
17.	The method of claim 15, wherein the plurality of services comprises audio, video or a combination thereof.	*See, e.g.*, *Johnson* at 10:18-21	
18.	The method according to claim 2, wherein the secure communication link is an authenticated link.	*See, e.g.*, *RFC 2401* at 4, 10	Request at §IX.A(17)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	*Claim Element*	*Relevant Provisions*	*Discussed further at:*
19.	The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.	*See, e.g., Johnson* at 6:17-19, Abstract, Figure 1	Request at §IX.A(18)
20.	The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.	*See, e.g., Johnson* at 6:17-19, Abstract, Figure 1	Request at §IX.A(19)
21.	The method according to claim 2, further including providing an unsecured name associated with the device.	*See, e.g., Johnson* at 1:21-27, 6:29-32, 11:23-24 *See, e.g., RFC 2131* at 3, 6, 8, 9, 26 *See, e.g., RFC 1034* at 11-12	Request at §IX.A(20)
22.	The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.	*See, e.g., Johnson* at 6:25-35, 9:23-33, 8:4-9, 10:36-52, 12:20-25, Figure 1 *See, e.g., RFC 2131* at 1-3	Request at §IX.A(21)
23.	The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.	*See, e.g., Johnson* at 6:25-35, 9:23-33, 8:4-9, 10:36-52, 12:20-25, Figure 1 *See, e.g., RFC 2131* at 1-3	Request at §IX.A(22)
24.	A method of using a first device to securely communicate with a second device over a communication network, the method comprising:	*See, e.g., Johnson* at 1:19-27, 10:36-50, ABSTRACT, Figure 1	Request at §IX(A)(23)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
24(a).	at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address	*See, e.g., Johnson* at 8:4-9, 9:23-33, 10:36-52, 12:20-25, Figure 1, Figure 3, Figure 5	Request at §IX(A)(23)
24(b).	receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device.	*See, e.g., Johnson* at 8:10-12	Request at §IX(A)(23)
24(c).	sending a message securely from the first device to the second device.	*See, e.g., Johnson* at 7:20-27	Request at §IX(A)(23)
25.	The method according to claim 24, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.	*See, e.g., Johnson* at 8:4-9, 9:23-33, 10:36-52, 12:20-25, Figure 1, Figure 3, Figure 5	Request at §IX(A)(24)
26.	A method of using a first device to communicate with a second device over a communication network, the method comprising:	*See, e.g., Johnson* at 1:19-27, 10:36-50, ABSTRACT, Figure 1	Request at §IX(A)(25)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
26(a).	from the first device requesting and obtaining registration of an unsecured name associated with the first device	*See, e.g., Johnson* at 6:23-35, 11:23-25, Figure 1 *See, e.g., RFC 2131* at 1-3, 6, 8-9, 26 *See, e.g., RFC 1034* at 11-12	Request at §IX(A)(25)
26(b).	from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device.	*See, e.g., Johnson* at 8:4-9, 9:23-33, 10:36-52, 12:20-25, 10:36-52, Figure 1, Figure 3, Figure 5	Request at §IX(A)(25)
26(c).	receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device	*See, e.g., Johnson* at 8:10-12	Request at §IX(A)(25)
26(d).	from the first device sending a message securely from the first device to the second device	*See, e.g., Johnson* at 7:20-27	Request at §IX(A)(25)
27(a).	The method of claim 26, wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device	*See, e.g., Johnson* at 1:19-27, 6:25-35, 8:4-9, 9:23-33, 10:36-52, 11:23-24, 12:20-25, Abstract, Figure 1, Figure 3 *See, e.g., RFC 2131* at 1-3, 6, 8-9, 26 *See, e.g., RFC 1034* at 11-12	Request at §IX(A)(26)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
27(b).	wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.	*See, e.g., Johnson* at 1:19-27, 6:25-35, 8:4-9, 9:23-33, 10:36-52, 11:23-24, 12:20-25, Abstract, Figure 1, Figure 3 *See, e.g., RFC 2131* at 1-3, 6, 8-9, 26 *See, e.g., RFC 1034* at 11-12	Request at §IX(A)(26)
28.	A, non-transitory machine-readable medium comprising instructions for:	*See, e.g., Johnson at* 1:19-27, 10:36-50, Abstract	Request at §IX(A)(27)
28(a)	sending a message to a secure name service, the message requesting a network address associated with a secure name of a device	*See, e.g., Johnson* at 11:21-37, Figure 7	Request at §IX(A)(27)
28(b).	receiving a message containing the network address associated with the secure name of the device	*See, e.g., Johnson* at 7:10-17	Request at §IX(A)(27)
28(c).	sending a message to the network address associated with the secure name of the device using a secure communication link.	*See, e.g., Johnson* at 7:20-27, 8:9-18	Request at §IX(A)(27)
29.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:	*See, e.g., Johnson at* 1:19-27, 10:36-50, Abstract	Request at §IX(A)(27)

Claim Chart – USP 8,051,181 relative to Johnson

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
29(a).	receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered	*See, e.g., Johnson* at 7:10-17, 8:10-12	Request at §IX(A)(27)
29(b).	sending a message securely from the first device to the second device.	*See, e.g., Johnson* at 7:20-27	Request at §IX(A)(27)

EXHIBIT C1

CLAIM CHART - '181 RELATIVE TO BESER

Claim Chart – USP 8,051,181 relative to Beser

Claim No.	*Claim Element*	*Relevant Provisions*	*Discussed further at:*
1.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising	*See, e.g., Beser* at 1:54-56, 4:5-11, 4:43-54, 10:37-41, 11:22-24, 11:26-37, 12:9-19, 25:42-26, Figure 1, Figure 5	Request at §IV(A)(1)
1(a).	receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device;	*See, e.g., Beser* at 1:54-56, 2:6-12, 2:35-40, 8:15-20, 11:20-25, 11:26-37, 11:59-62, 12:28-36, Figure 6	Request at §IV(A)(1)
1(b).	sending a message over a secure communication link from the first device to the second device.	*See, e.g., Beser* at 4:43-54, Figure 17	Request at §IV(A)(1)
2.	[a] method of using a first device to communicate with a second device having a secure name, the method comprising:	*See, e.g., Beser* at 4:5-11, 4:43-44, 4:47-50, 25:42-26, 10:37-41, 11:28-32, Figure 1	Request at §IV(A)(2)
2(a).	from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;	*See, e.g., Beser* at 4:5-11, 10:2-6, 11:9-10, 11:25-29, 11:59-62, Figure 7	Request at §IV(A)(2)
2(b).	at the first device, receiving a message containing the network address associated with the secure name of the second device;	*See, e.g., Beser* at 21:38-43	Request at §IV(A)(2)

Claim Chart – USP 8,051,181 relative to Beser

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
2(c).	from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.	*See, e.g., Beser* at 4:43-54, Figure 17	Request at §IV(A)(2)
3.	The method according to claim 2, wherein the secure name of the second device is a secure domain name.	*See, e.g., Beser* at 10:38-41	Request at §IV(A)(3)
4.	The method according to claim 2, wherein the secure name indicates security.	*See, e.g., Beser* at 11:13-25	Request at §IV(A)(4)
5.	The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.	*See, e.g., Beser* at 1:54-56, 2:6-12, 12:6-19	Request at §IV(A)(5)
6.	The method according to claim 5, further including decrypting the message.	*See, e.g., Beser* at 1:54-56, 2:6-12, 12:6-19	Request at §IV(A)(6)
7.	The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.	*See, e.g., Beser* at 4:55-63	Request at §IV(A)(7)

Claim Chart – USP 8,051,181 relative to Beser

Claim No.	*Claim Element*	*Relevant Provisions*	*Discussed further at:*
8.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device	*See, e.g., Beser* at 21:38-43	Request at §IV(A)(8)
9.	The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.	*See, e.g., Beser* at 4:5-11, 4:43-44, 4:47-50, 25:42-26, 10:37-41, 11:28-32, Figure 1	Request at §IV(A)(9)
10.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.	*See, e.g., Beser* at 2:6-12, 6:58-59, 12:6-19	Request at §IV(A)(10)
11.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.	*See, e.g., Beser* at 2:6-12, 6:58-59, 12:6-19	Request at §IV(A)(11)
12.	The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols	*See, e.g., Beser* at 5:49 – 7:60, Figure 2	Request at §IV(A)(12)

Claim Chart – USP 8,051,181 relative to Beser

Claim No.	*Claim Element*	*Relevant Provisions*	*Discussed further at:*
13.	The method according to claim 2, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.	*See, e.g., Beser* at 4:43-54	Request at §IV(A)(13)
14.	The method according to claim 2, further including supporting a plurality of services over the secure communication link.	*See, e.g., Beser* at 4:43-54	Request at §IV(A)(14)
15.	The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.	*See, e.g., Beser* at 4:43-54, 5:49 – 7:60, Figure 2	Request at §IV(A)(15)
16.	The method of claim 15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.	*See, e.g., Beser* at 4:43-54	Request at §IV(A)(16)
17.	The method of claim 15, wherein the plurality of services comprises audio, video or a combination thereof.	*See, e.g., Beser* at 4:43-54	Request at §IV(A)(17)
18.	The method according to claim 2, wherein the secure communication link is an authenticated link.	*See, e.g., Beser* at 1:54–2:15, 11:22-24 *See, e.g., RFC 2401* at 30-31	Request at §IV(A)(18) Request at §IV(B)(1)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
19.	The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.	*See, e.g., Beser* at 4:43-54	Request at §IV(A)(19)
20.	The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.	*See, e.g., Beser* at 4:43-54	Request at §IV(A)(20)
21.	The method according to claim 2, further including providing an unsecured name associated with the device.	*See, e.g., Beser* at 11:25-32	Request at §IV(A)(21)
22.	The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.	*See, e.g., Beser* at 10:45-48	Request at §IV(A)(22)
23.	The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.	*See, e.g., Beser* at 10:38-41	Request at §IV(A)(23)
24.	A method of using a first device to securely communicate with a second device over a communication network, the method comprising:	*See, e.g., Beser* at 3:1-10	Request at §IV(A)(24)
24(a).	at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address	*See, e.g., Beser* at 10:45-48	Request at §IV(A)(24)

Claim Chart – USP 8,051,181 relative to Beser

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
24(b).	receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device.	*See, e.g.*, *Beser* at 1:54-56, 2:6-12, 2:35-40, 8:15-20, 11:20-25, 11:26-37, 11:59-62, 12:28-36, Figure 6	Request at §IV(A)(24)
24(c).	sending a message securely from the first device to the second device.	*See, e.g.*, *Beser* at 4:43-54, Figure 17	Request at §IV(A)(24)
25.	The method according to claim 24, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.	*See, e.g.*, *Beser* at 4:43-54, 10:45-48, Figure 17	Request at §IV(A)(25)
26.	A method of using a first device to communicate with a second device over a communication network, the method comprising:	*See, e.g.*, *Beser* at 3:1-10	Request at §IV(A)(26)
26(a).	from the first device requesting and obtaining registration of an unsecured name associated with the first device	*See, e.g.*, *Beser* at 11:25-32	Request at §IV(A)(26)
26(b).	from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device.	*See, e.g.*, *Beser* at 10:45-48	Request at §IV(A)(26)

Claim Chart – USP 8,051,181 relative to Beser

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
26(c).	receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device	*See, e.g.*, *Beser* at 1:54-56, 2:6-12, 2:35-40, 8:15-20, 11:20-25, 11:26-37, 11:59-62, 12:28-36, Figure 6	Request at §IV(A)(27)
26(d).	from the first device sending a message securely from the first device to the second device	*See, e.g.*, *Beser* at 4:43-54, Figure 17	Request at §IV(A)(27)
27(a).	The method of claim 26, wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device	*See, e.g.*, *Beser* at 11:25-32	Request at §IV(A)(27)
27(b).	wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.	*See, e.g.*, *Beser* at 10:45-48	Request at §IV(A)(27)
28.	A, non-transitory machine-readable medium comprising instructions for:	*See, e.g.*, *Beser* at 25:42-26	Request at §IV(A)(28)
28(a)	sending a message to a secure name service, the message requesting a network address associated with a secure name of a device	*See, e.g.*, *Beser* at 4:5-11, 10:2-6, 11:9-10, 11:25-29, 11:59-62, Figure 7	Request at §IV(A)(28)
28(b).	receiving a message containing the network address associated with the secure name of the device	*See, e.g.*, *Beser* at 21:38-43	Request at §IV(A)(28)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
28(c).	sending a message to the network address associated with the secure name of the device using a secure communication link.	*See, e.g., Beser* at 4:43-54, Figure 17	Request at §IV(A)(28)
29.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:	*See, e.g., Beser* at 4:5-11, 4:43-44, 4:47-50, 10:37-41, 11:28-32, 25:42-26, Figure 1	Request at §IV(A)(29)
29(a).	receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered	*See, e.g., Beser* at 1:54-56, 2:6-12, 2:35-40, 8:15-20, 10:45-48, 11:20-25, 11:26-37, 11:59-62, 12:28-36, Figure 6	Request at §IV(A)(29)
29(b).	sending a message securely from the first device to the second device.	*See, e.g., Beser* at 4:43-54, Figure 17	Request at §IV(A)(29)

EXHIBIT C3

CLAIM CHART - '181 RELATIVE TO LENDENMANN

Claim Chart – USP 8,051,181 relative to Lendenmann

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
1.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising	*See, e.g.*, *Lendenmann* at 1, 8-10, 21-24, 34, Figure 9, Figure 10	Request at § VI.A(1)
1(a).	receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device;	*See, e.g.*, *Lendenmann* at 173, 174, 178, 179, 182, 191, 192, Figure 68	Request at § VI.A(1)
1(b).	sending a message over a secure communication link from the first device to the second device.	*See, e.g.*, *Lendenmann* at 71, 192	Request at § VI.A(1)
2.	[a] method of using a first device to communicate with a second device having a secure name, the method comprising:	*See, e.g.*, *Lendenmann* at 1, 8-10, 22-24, Figure 10	Request at § VI.A(2)
2(a).	from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;	*See, e.g.*, *Lendenmann* at 21, 34, 173, 174, 178, 179, 182	Request at § VI.A(2)
2(b).	at the first device, receiving a message containing the network address associated with the secure name of the second device;	*See, e.g.*, *Lendenmann* at 191, Figure 68	Request at § VI.A(2)
2(c).	from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.	*See, e.g.*, *Lendenmann* at 71, 192	Request at § VI.A(2)

Claim Chart – USP 8,051,181 relative to Lendenmann

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
3.	The method according to claim 2, wherein the secure name of the second device is a secure domain name.	*See, e.g.*, *Lendenmann* at 23, 24, 28, Figure 9, Figure 11	Request at § VI.A(3)
4.	The method according to claim 2, wherein the secure name indicates security.	*See, e.g.*, *Lendenmann* at 10	Request at § VI.A(4)
5.	The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.	*See, e.g.*, *Lendenmann* at 21, 34, 57, 182, 186, 192	Request at § VI.A(5)
6.	The method according to claim 5, further including decrypting the message.	*See, e.g.*, *Lendenmann* at 21, 34, 57, 182, 186, 192	Request at § VI.A(6)
7.	The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.	*See, e.g.*, *Lendenmann* at 192	Request at § VI.A(7)
8.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device	*See, e.g.*, *Lendenmann* at 181, Figure 66	Request at § VI.A(8)

Claim Chart – USP 8,051,181 relative to Lendenmann

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
9.	The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.	*See, e.g., Lendenmann* at 9	Request at § VI.A(9)
10.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.	*See, e.g., Lendenmann* at 192 *See, e.g., Beser* at 2:6-12, 6:58-59, 12:6-19 *See, e.g., RFC2401* at 4-5, 24-26	Request at §VI.B(3)(a) and §VI.B(4)(a)
11.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.	*See, e.g., Lendenmann* at 192 *See, e.g., Beser* at 2:6-12, 6:58-59, 12:6-19 *See, e.g., RFC2401* at 4-5, 24-26	Request at §VI.B(3)(b) and §VI.B(4)(b)
12.	The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols	*See, e.g., Lendenmann* at 179-180	Request at § VI.A(10)
13.	The method according to claim 2, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.	*See, e.g., Lendenmann* at 100, 176	Request at § VI.A(11)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
14.	The method according to claim 2, further including supporting a plurality of services over the secure communication link.	*See, e.g., Lendenmann* at 178-179	Request at § VI.A(12)
15.	The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.	*See, e.g., Lendenmann* at 179-180	Request at § VI.A(13)
16.	The method of claim 15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.	*See, e.g., Beser* at 4:43-54	Request at § VI.B(c)
17.	The method of claim 15, wherein the plurality of services comprises audio, video or a combination thereof.	*See, e.g., Beser* at 4:43-54	Request at § VI.B(d)
18.	The method according to claim 2, wherein the secure communication link is an authenticated link.	*See, e.g., Lendenmann* at 34, 57	Request at § VI.A(14)
19.	The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.	*See, e.g., Lendenmann* at 57	Request at § VI.A(15)

Claim Chart – USP 8,051,181 relative to Lendenmann

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
20.	The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.	*See, e.g., Lendenmann* at 57	Request at § VI.A(16)
21.	The method according to claim 2, further including providing an unsecured name associated with the device.	*See, e.g., Lendenmann* at 22, 23	Request at § VI.A(17)
22.	The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.	*See, e.g., Lendenmann* at 34, 178-179, 203	Request at § VI.A(18)
23.	The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.	*See, e.g., Lendenmann* at 23, 181, Figure 9, Figure 66	Request at § VI.A(19)
24.	A method of using a first device to securely communicate with a second device over a communication network, the method comprising:	*See, e.g., Lendenmann* at 1, 8-10, 22-24, Figure 9, Figure 10	Request at § VI.A(20)
24(a).	at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address	*See, e.g., Lendenmann* at 34, 178-179, 203	Request at § VI.A(20)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
24(b).	receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device.	*See, e.g.*, *Lendenmann* at 173, 174, 178, 179, 182, 191, 192, Figure 68	Request at § VI.A(20)
24(c).	sending a message securely from the first device to the second device.	*See, e.g.*, *Lendenmann* at 71, 192	Request at § VI.A(20)
25.	The method according to claim 24, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.	*See, e.g.*, *Lendenmann* at 71, 178, 179, 192, 203	Request at § VI.A (21)
26.	A method of using a first device to communicate with a second device over a communication network, the method comprising:	*See, e.g.*, *Lendenmann* at 1, 8-10, 22, 23, Figure 9, Figure 10	Request at § VI.A(22)
26(a).	from the first device requesting and obtaining registration of an unsecured name associated with the first device	*See, e.g.*, *Lendenmann* at 24	Request at § VI.A(22)
26(b).	from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device.	*See, e.g.*, *Lendenmann* at 178-179, 203	Request at § VI.A(22)

Claim Chart – USP 8,051,181 relative to Lendenmann

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
26(c).	receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device	*See, e.g.*, *Lendenmann* at 173, 174, 178, 179, 182, 191, 192, Figure 68	Request at § VI.A(22)
26(d).	from the first device sending a message securely from the first device to the second device	*See, e.g.*, *Lendenmann* at 71, 192	Request at § VI.A(22)
27(a).	The method of claim 26, wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device	*See, e.g.*, *Lendenmann* at 24	Request at § VI.A(23)
27(b).	wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.	*See, e.g.*, *Lendenmann* at 178-179, 203	Request at § VI.A(23)
28.	A, non-transitory machine-readable medium comprising instructions for:	*See, e.g.*, *Lendenmann* at 1	Request at § VI.A(24)
28(a)	sending a message to a secure name service, the message requesting a network address associated with a secure name of a device	*See, e.g.*, *Lendenmann* at 8-10, 22-24, 173, 174, 178, 179, 182, Figure 9, Figure 10	Request at § VI.A(24)
28(b).	receiving a message containing the network address associated with the secure name of the device	*See, e.g.*, *Lendenmann* at 191, Figure 68	Request at § VI.A(24)

Claim Chart – USP 8,051,181 relative to Lendenmann

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
28(c).	sending a message to the network address associated with the secure name of the device using a secure communication link.	*See, e.g.*, *Lendenmann* at 71, 192	Request at § VI.A(24)
29.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:	*See, e.g.*, *Lendenmann* at 1, 8-10, 22-24, 34, Figure 9, Figure 10	Request at § VI.A(25)
29(a).	receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered	*See, e.g.*, *Lendenmann* at 173, 174, 178, 179, 182, 191, 192, Figure 68	Request at § VI.A(25)
29(b).	sending a message securely from the first device to the second device.	*See, e.g.*, *Lendenmann* at 71, 192	Request at § VI.A(25)

EXHIBIT C4

CLAIM CHART - '181 RELATIVE TO PROVINO

Claim Chart – USP 8,051,181 relative to Provino

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
1.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising	*See, e.g.*, *Provino* at 1:56-60, 8:67-9:5, 8:40-43, 9:17-27, 9: 32–10:13, 10:45-52, 10:54-56, 10:62-67, 13:26-67, Figure 1	Request at § VIII.A(1)
1(a).	receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device;	*See, e.g.*, *Provino* at 9:46-52.	Request at § VII.A(1)
1(b).	sending a message over a secure communication link from the first device to the second device.	*See, e.g.*, *Provino* at 9:32-44.	Request at § VII.A(1)
2.	[a] method of using a first device to communicate with a second device having a secure name, the method comprising:	*See, e.g.*, *Provino* at 1:56-60, 8:67-9:5, 8:40-43, 9:2-5, 9:17-27, 9: 32–10:13, 10:45-52, 10:54-56, 10:62-67, 13:26-67, Figure 1	Request at § VII.A(2)
2(a).	from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;	*See, e.g.*, *Provino* at 13:54-67.	Request at § VII.A(2)
2(b).	at the first device, receiving a message containing the network address associated with the secure name of the second device;	*See, e.g.*, *Provino* at 14:39-46, 14:57-63.	Request at § VII.A(2)
2(c).	from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.	*See, e.g.*, *Provino* at 9:32-44.	Request at § VII.A(2)

Claim Chart – USP 8,051,181 relative to Provino

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
3.	The method according to claim 2, wherein the secure name of the second device is a secure domain name.	*See, e.g., Provino* at 1:56-60.	Request at § VII.A(3)
4.	The method according to claim 2, wherein the secure name indicates security.	*See, e.g., Provino* at 9:32-36, 9:52-56.	Request at § VII.A(4)
5.	The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.	*See, e.g., Provino* at 9:60-10:13,10:25-27.	Request at § VII.A(5)
6.	The method according to claim 5, further including decrypting the message.	*See, e.g., Provino* at 9:60-10:13,10:25-27.	Request at § VII.A(6)
7.	The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.	*See, e.g., Provino* at 9:32-52	Request at § VII.A(7)
8.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device	*See, e.g., Provino* at 14:39-46, 14:57-63.	Request at § VII.A(8)

Claim Chart – USP 8,051,181 relative to Provino

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
9.	The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.	*See, e.g.*, *Provino* at 1:56-60, 8:67-9:5, 8:40-43, 9:2-5, 9:17-27, 9: 32–10:13, 10:45-52, 10:54-56, 10:62-67, 13:26-67, Figure 1	Request at § VII.A(9)
10.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.	*See, e.g.*, *Provino* at 14:39-46, 14:57-63.	Request at § VII.A(10)
11.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.	*See, e.g.*, *Provino* at 9:32-44.	Request at § VII.A(11)
12.	The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols	*See, e.g.*, *Provino* at 5:10-13, 5:28-32.	Request at § VII.A(12)
13.	The method according to claim 2, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.	*See, e.g.*, *Provino* at 5:10-13, 5:28-32.	Request at § VII.A(13)

Claim Chart – USP 8,051,181 relative to Provino

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
14.	The method according to claim 2, further including supporting a plurality of services over the secure communication link.	*See, e.g.*, *Provino* at 5:10-13, 5:28-32.	Request at § VII.A(14)
15.	The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.	*See, e.g.*, *Provino* at 5:10-13, 5:28-32.	Request at § VII.A(15)
16.	The method of claim 15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.	*See, e.g.*, *Provino* at 5:10-13, 5:28-32.	Request at § VII.A(16)
17.	The method of claim 15, wherein the plurality of services comprises audio, video or a combination thereof.	*See, e.g.*, *Provino* at 5:10-13, 5:28-32.	Request at § VII.A(17)
18.	The method according to claim 2, wherein the secure communication link is an authenticated link.	*See, e.g.*, *Provino* at 9:46-60, 9:56-10:12.	Request at § VII.A(18)
19.	The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.	*See, e.g.*, *Provino* at 6:19-23, 9:52-65, 10:45–11:25.	Request at § VII.A(19)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
20.	The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.	*See, e.g., Provino* at 6:19-23, 9:52-65, 10:45–11:25.	Request at § VII.A(20)
21.	The method according to claim 2, further including providing an unsecured name associated with the device.	*See, e.g., Provino* at Figure 1.	Request at § VII.A(21)
22.	The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.	*See, e.g., Provino* at 1:56-60, 8:67-9:5, 8:40-43, 9:2-5, 9:17-27, 9: 32–10:13, 10:45-52, 10:54-56, 10:62-67, 13:26-67, Figure 1	Request at § VII.A(22)
23.	The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.	*See, e.g., Provino* at 1:56-60, 8:67-9:5, 8:40-43, 9:2-5, 9:17-27, 9: 32–10:13, 10:45-52, 10:54-56, 10:62-67, 13:26-67, Figure 1	Request at § VII.A(23)
24.	A method of using a first device to securely communicate with a second device over a communication network, the method comprising:	*See, e.g., Provino* at 1:56-60, 8:67-9:5, 9:17-27, 9:32-10:13, 10:45-52, 13:26-67, Figure 1	Request at § VII.B(3)
24(a).	at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address	*See, e.g., H.323* at 7-8, 27, 33-35, 38	Request at § VII.B(3)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
24(b).	receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device.	*See, e.g., Provino* at 9:46-52	Request at § VII.B(3)
24(c).	sending a message securely from the first device to the second device.	*See, e.g., Provino* at 9:32-44	Request at § VII.B(3)
25.	The method according to claim 24, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.	*See, e.g., Provino* at 9:32-44, Figure 1	Request at § VII.B(4)
26.	A method of using a first device to communicate with a second device over a communication network, the method comprising:	*See, e.g., Provino* at Abstract	Request at § VII.B(5)
26(a).	from the first device requesting and obtaining registration of an unsecured name associated with the first device	*See, e.g., H.323* at 7-8, 27, 33-35, 38	Request at § VII.B(5)
26(b).	from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device.	*See, e.g., H.323* at 7-8, 27, 33-35, 38	Request at § VII.B(5)

Claim Chart – USP 8,051,181 relative to Provino

Claim No.	*Claim Element*	*Relevant Provisions*	*Discussed further at:*
26(c).	receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device	*See, e.g., H.323* at 6, 30-31, 38, 81	Request at § VII.B(5)
26(d).	from the first device sending a message securely from the first device to the second device	*See, e.g., H.323* at 6	Request at § VII.B(5)
27(a)	The method of claim 26, wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device	*See, e.g., H.323* at 35	Request at § VII.B(6)
27(b)	Wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device	*See, e.g., H.323* at 35, 38	Request at § VII.B(6)
28.	A, non-transitory machine-readable medium comprising instructions for:	*See, e.g., Provino* at 6:19-23, 9:52-65, 10:45-11:25	Request at § VII.A(24)
28(a)	sending a message to a secure name service, the message requesting a network address associated with a secure name of a device	*See, e.g., Provino* at 9:56-10:7	Request at § VII.A(24)

Claim Chart – USP 8,051,181 relative to Provino

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
28(b).	receiving a message containing the network address associated with the secure name of the device	*See, e.g., Provino* at 14:39-46, 57-63	Request at § VII.A(24)
28(c).	sending a message to the network address associated with the secure name of the device using a secure communication link.	*See, e.g., Provino* at 9:32-44, Figure 1	Request at § VII.A(24)
29.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:	*See, e.g., Provino* at 1:56-60, 8:67-9:5, 9:17-27, 9:32-10:13, 10:45-52, 13:26-67, Figure 1	Request at § VII.A(25)
29(a).	receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered	*See, e.g., Provino* at 9:46-52, 9:56-10:7	Request at § VII.A(25)
29(b).	sending a message securely from the first device to the second device.	*See, e.g., Provino* at 9:32-44, Figure 1	Request at § VII.A(25)

EXHIBIT C5

CLAIM CHART - '181 RELATIVE TO H.323

Claim Chart – USP 8,051,181 relative to H.323

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
1.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising	*See, e.g., H.323* at 2, 5-6, 7-8, 27, 33-35, 38, Figure 1 *See, e.g., H.225* at 141-143	Request at § VIII(A)(1)
1(a).	receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device;	*See, e.g., H.323* at 38 *See, e.g., H.235* at 6-7, 28-29, 30-31	Request at § VIII(A)(1)
1(b).	sending a message over a secure communication link from the first device to the second device.	*See, e.g., H.323* at 38 *See, e.g., H.235* at 6-7, 28-29, 30-31	Request at § VIII(A)(1)
2.	[a] method of using a first device to communicate with a second device having a secure name, the method comprising:	*See, e.g., H.323* at 8, 27, 28, 34, 38, Figure 3 *See, e.g., H.235* at 6-7, 28-29, 30-31	Request at § VIII(A)(2)
2(a).	from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;	*See, e.g., H.323* at 8, 27, 28, 34, 38, Figure 3 *See, e.g., H.235* at 28-29, 30-31	Request at § VIII(A)(2)
2(b).	at the first device, receiving a message containing the network address associated with the secure name of the second device;	*See, e.g., H.323* at 38 *See, e.g., H.235* at 28, 30-31	Request at § VIII(A)(2)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
2(c).	from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.	*See, e.g., H.235* at 6-7, 30-31	Request at § VIII(A)(2)
3.	The method according to claim 2, wherein the secure name of the second device is a secure domain name.	*See, e.g., H.323* at 33-34	Request at § VIII(A)(3)
4.	The method according to claim 2, wherein the secure name indicates security.	*See, e.g., H.235* at 28	Request at § VIII(A)(4)
5.	The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.	*See, e.g., H.235* at 30	Request at § VIII(A)(5)
6.	The method according to claim 5, further including decrypting the message.	*See, e.g., H.235* at 30-31	Request at § VIII(A)(6)
7.	The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.	*See, e.g., H.235* at 8	Request at § VIII(A)(7)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
8.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device	*See, e.g.*, *H.323* at 7-8	Request at § VIII(A)(8)
9.	The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.	*See, e.g.*, *H.323* at 8, 27, 28, 34, 38, Figure 3 *See, e.g.*, *H.235* at 6-7, 28-29, 30-31	Request at § VIII(A)(9)
10.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.	*See, e.g.*, *H.235* at 30-31	Request at § VIII(A)(10)
11.	The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.	*See, e.g.*, *H.323* at 8, 27, 28, 34, 38, Figure 3 *See, e.g.*, *H.235* at 6-7, 28-29, 30-31	Request at § VIII(A)(11)
12.	The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols	*See, e.g.*, *H.323* at 14, 96 *See, e.g.*, *H.235* at 20	Request at § VIII(A)(12)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
13.	The method according to claim 2, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.	*See, e.g.*, *H.323* at 91 *See, e.g.*, *H.225* at 73	Request at § VIII(A)(13)
14.	The method according to claim 2, further including supporting a plurality of services over the secure communication link.	*See, e.g.*, *H.323* at 14, 25 *See, e.g.*, *H.225* at 73	Request at § VIII(A)(14)
15.	The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.	*See, e.g.*, *H.323* at 14, 25	Request at § VIII(A)(15)
16.	The method of claim 15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.	*See, e.g.*, *H.323* at (i), 4-5, 13, 79	Request at § VIII(A)(16)
17.	The method of claim 15, wherein the plurality of services comprises audio, video or a combination thereof.	*See, e.g.*, *H.323* at (i), 4-5, 13, 79	Request at § VIII(A)(17)
18.	The method according to claim 2, wherein the secure communication link is an authenticated link.	*See, e.g.*, *H.235* at 30-31	Request at § VIII(A)(18)

Claim Chart – USP 8,051,181 relative to H.323

Claim No.	*Claim Element*	*Relevant Provisions*	*Discussed further at:*
19.	The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.	*See, e.g., H.323* at (i)	Request at § VIII(A)(19)
20.	The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.	*See, e.g., H.323* at (i)	Request at § VIII(A)(20)
21.	The method according to claim 2, further including providing an unsecured name associated with the device.	*See, e.g., H.323* at 2, 5-6, 33-35 *See, e.g., H.225* at 141-143	Request at § VIII(A)(21)
22.	The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.	*See, e.g., H.323* at 35	Request at § VIII(A)(22)
23.	The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.	*See, e.g., H.323* at 33-34	Request at § VIII(A)(23)
24.	A method of using a first device to securely communicate with a second device over a communication network, the method comprising:	*See, e.g., H.323* at 1.	Request at §VIII(A)(24)
24(a).	at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address	*See, e.g., H.323* at 7-8, 27, 33-35, 38	Request at §VIII(A)(24)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
24(b).	receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device.	*See, e.g., H.323* at 38, 81 *See, e.g., H.235* at 6, 30-31	Request at §VIII(A)(24)
24(c).	sending a message securely from the first device to the second device.	*See, e.g., H.235* at 6	Request at §VIII(A)(24)
25.	The method according to claim 24, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.	*See, e.g., H.323* at 35, 38	Request at §VIII(A)(25)
26.	A method of using a first device to communicate with a second device over a communication network, the method comprising:	*See, e.g., H.323* at 1	Request at §VIII(A)(26)
26(a).	from the first device requesting and obtaining registration of an unsecured name associated with the first device	*See, e.g., H.323* at 33-35, 38	Request at § VIII(A)(26)
26(b).	from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device.	*See, e.g., H.323* at 2, 5-6, 33-35, 38 *See, e.g., H.225.0* at 45	Request at § VIII(A)(26)

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
26(c).	receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device	*See, e.g., H.323* at 38, 81 *See, e.g., H.235* at 6, 30-31	Request at § VIII(A)(26)
26(d).	from the first device sending a message securely from the first device to the second device	*See, e.g., H.235* at 6	Request at § VIII(A)(26)
27(a).	The method of claim 26, wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device	*See, e.g., H.323* at 35	Request at § VIII(A)(27)
27(b).	wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.	*See, e.g., H.323* at 35, 38	Request at § VIII(A)(27)
28.	A, non-transitory machine-readable medium comprising instructions for:	*See, e.g., H.323* at 1	Request at § VIII(A)(28)
28(a)	sending a message to a secure name service, the message requesting a network address associated with a secure name of a device	*See, e.g., H.323* at 8, 27, 34	Request at § VIII(A)(28)
28(b).	receiving a message containing the network address associated with the secure name of the device	*See, e.g., H.235* at 30	Request at § VIII(A)(28)

Claim Chart – USP 8,051,181 relative to H.323

Claim No.	***Claim Element***	***Relevant Provisions***	***Discussed further at:***
28(c).	sending a message to the network address associated with the secure name of the device using a secure communication link.	*See, e.g., H.235* at 6-7, 30-31	Request at § VIII(A)(28)
29.	A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:	*See, e.g., H.323* at 1	Request at § VIII(A)(29)
29(a).	receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered	*See, e.g., H.235* at 6-7, 30-31	Request at § VIII(A)(29)
29(b).	sending a message securely from the first device to the second device.	*See, e.g., H.235* at 6-7, 30-31	Request at § VIII(A)(29)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 8,051,181		)	
		)	
Filed:	February 27, 2007	)	Group Art Unit: Central Reexamination Unit
		)	
Issued:	November 1, 2011	)	
		)	Examiner:
Inventors:	Larson et al.	)	
		)	Confirmation No.:
For:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	

REQUEST FOR INTER PARTES REEXAMINATION UNDER 35 U.S.C. § 311

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir,

Presented herewith is a request for *inter partes* reexamination of United States Patent No. 8,051,181 (the '181 patent), entitled "Method for Establishing Secure Communication Link Between Computers of Virtual Private Network." The inventors of the '181 patent are Victor Larson, Robert Dunham Short, Edmund Colby Munger, and Michael Williamson. The present assignee of the '181 patent is VirnetX Corporation, as recorded at Reel 019464, Frame 0133. A list of all exhibits submitted with this reexamination request is provided in the accompanying transmittal letter for this request for inter partes reexamination.

TABLE OF CONTENTS

Exhibit List

A	U.S. Patent 8,051,181
B	Certificate of Service
C1	Claim Chart – Beser
C2	Claim Chart – Mattaway
C3	Claim Chart – Lendenmann
C4	Claim Chart – Provino
C5	Claim Chart – H.323
C6	Claim Chart – Johnson
X1	U.S. Patent No. 6,496,867 to Beser
X2	U.S. Patent No. 6,131,121 to Mattaway
X3	Lendenmann, "Understanding OSF DCE 1.1 for AIX and OS/2," (October 1995)
X4	U.S. Patent No. 6,557,037 to Provino
X5	Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," November 1987
X6	U.S. Patent No. 6,499,108 to Johnson
X7	ITU-T H.323, "Packet-based multimedia communications systems," February 1998
X8	ITU-T H.225.0, "Call signaling protocols and media stream packetization for packet-based multimedia communication systems," February 1998
X9	ITU-T H.235, "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," November 1998
X10	ITU-T H.245, "Infrastructure of audiovisual services – Communication procedures," February 1998
X11	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987

I. COMPLIANCE WITH REQUIREMENTS FOR A REQUEST FOR *INTER PARTES* REEXAMINATION

A. The '181 Patent is Eligible to be the Subject of an Inter Partes Reexamination

The '181 patent issued on November 1, 2011 from U.S. Application No. 11/679,416, which was filed on February 27, 2007. The '181 patent, thus, was issued from an original application filed on or after November 29, 1999, in compliance with 37 C.F.R. § 1.913. This request is being made during the period of enforceability of the '181 patent.

B. Claims of the '181 Patent for which Reexamination is Requested

Pursuant to 37 CFR 1.915(b)(1), the claims of the '181 patent for which reexamination is requested are claims 1 to 29 of the '181 patent.

C. Fee for Reexamination

The Director is authorized to charge the fee specified in 37 C.F.R. § 1.20(c)(2) to Deposit Account No. 18-1260.

D. Citation and Copies of Patents and Printed Publications that Establish a Substantial New Question of Patentability

Pursuant to 37 CFR 1.915(b)(2), a citation of the patents and printed publications presented to establish a reasonable basis for prevailing in this reexamination are listed on the accompanying form PTO/SB/42. Pursuant to 37 CFR 1.915(b)(4), a complete copy of each patent and printed publication cited on the PTO Form SB/42 is also provided herewith.

E. Copy of the Patent For Which Reexamination is Requested

In compliance with 37 C.F.R. § 1.915(b)(4) and (5), a complete copy of the '181 patent is provided as **Exhibit A**.

F. Certificate of Service by Requester on the Patent Owner

Exhibit B is a copy of the certificate of service used to effect service of the entirety of this request for reexamination on the owner of the '181 patent. Service on the patent owner has been effected at the address specified for that patent owner under 37 CFR 1.33(c); namely:

VirnetX Inc.
c/o McDermott Will & Emery
600 13th Street, N.W.
Washington, D.C. 20005-3096

G. Real Party of Interest of the Requester

The real party of interest of the Requester of this request for inter partes reexamination is Apple Inc. ("Apple"), located at 1 Infinite Loop, Cupertino, CA 95014.

H. Certification that Requester is Not Estopped from Requesting Reexamination

Requester hereby certifies that the estoppel provisions of § 1.907 do not prohibit inter partes reexamination of the '181 patent based upon this request for the following reasons:

(i) This request complies with 37 CFR 1.907(a), as the real party of interest of the Requestor, Apple, has not previously requested reexamination of the '181 patent.

(ii) This request complies with 37 CFR 1.907(b) as there has been no final decision entered against Apple, or against a party in privity with Apple, in a civil action arising in whole or in part under 28 U.S.C. § 1338 involving any claim of the '181 patent.

(iii) This request complies with 37 CFR 1.907(c), as there has been no prior reexamination proceeding involving the '181 patent which was commenced in response to a request for inter partes reexamination filed by Apple, or by an entity in privity with Apple.

(iv) Requester certifies that Apple is not in privity with and has no commercial relationship to the owner of the '181 patent, VirnetX, Inc.

II. STATEMENT IDENTIFYING EACH GROUND UPON WHICH REQUESTER IS LIKELY TO PREVAIL

A. Effective Filing Date of Claims 1-29 of the '181 Patent Is No Earlier than April 20, 2000

The '181 patent issued from U.S. Application No. 11/679,416, filed February 27, 2007. The '416 application is a continuation of U.S. Application No. 10/702,486, filed on November 7, 2003, now U.S. Patent No. 7,188,180, which is a division of U.S. Application No. 09/558,209, filed on April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, which is a continuation-in-part of U.S. application No. 09/429,643, filed on October 29, 1999, now U.S. Patent No. 7,010,604. The '416, '209, '783 and '643 applications each claim priority under 35 U.S.C. 119(e) to Provisional Application Nos. 60/106,261, filed October 30, 1998 and 60/137,704, filed June 7, 1998.

Claims 1, 2, 24, 26, 28, and 29 of the '181 patent are independent claims. Claims 3-23 depend from claim 2, claim 25 depends from claim 24, and claim 27 depends from claim 26. Consequently, claims 3-23, 25, and 27 cannot enjoy an effective filing date earlier than that of claims 2, 24, and 26, respectively, from which they depend.

Claims 1, 2, 24, 26, 28, and 29 of the '181 patent rely on information found only in the disclosures of the '416, '486, or '209 applications, and not found in any prior application to which the '181 patent claims benefit under 35 U.S.C. § 120 or priority under 35 U.S.C. § 119(e). For example, claim 1 of the '181 patent specifies "receiving, at a network address corresponding to the secure name associated with the first device." Similarly, claim 2 of the '181 patent describes "sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device." Additionally, each of independent claims 24, 26, 28 and 29 also describe a "secure name" or a "secure name service."

For these limitations, the claims of the '181 patent can only arguably rely on descriptions found solely in the '416, '486, or '209 applications. As a preliminary matter, it should be noted that none of the specifications in the '416, '486, or '209 applications explicitly describes the claimed "secure name" and "secure name service" of the '181 patent. Indeed, only those applications—and none before—describe a "secure domain name service," which, based on the prosecution history of the '181 patent, is purportedly a subset of the "secure name service." To the extent that there is any written description support for these concepts, the first appearance of such support for the claimed subject matter would have first appeared in the continuation-in-part U.S. Application No. 09/558,209, filed April 26, 2000. The '209 application includes a section labeled "CONTINUATION-IN-PART IMPROVEMENTS," beginning at page 56 of the originally-filed specification. This section includes, for example, a discussion of "querying a secure domain name service (SDNS)." So, because none of the '643 or '135 applications disclose or suggest a secure domain name service or secure domain name, these earlier filed applications to which the '181 patent claims benefit or priority therefore do not describe or enable the subject matter defined by at least claims 1, 2, 24, 26, 28, and 29 of the '181 patent.

Accordingly, the effective filing date for claims 1-29 of the '181 patent is no earlier than the filing date of the abandoned '209 application, April 26, 2000.

B. Prior Art Status of Cited Patents and Publications Upon Which Reexamination is Requested

Several substantial new questions of patentability are based on printed publications. The effective date of these publications is as follows:

1. Exhibit X1 – U.S. Patent No. 6,496,867 to Beser et al. ("Beser ")

Beser was filed August 27, 1999 and issued on December 17, 2002, and is prior art to the '181 patent under 35 U.S.C. § 102(e).

2. Exhibit X2 – U.S. Patent No. 6,131,121 to Mattaway et al. ("Mattaway")

Mattaway was filed on September 25, 1996 and issued October 10, 2000, and is prior art to the '181 patent under 35 U.S.C. § 102(e).

3. Exhibit X3 – Lendenmann, "Understanding OSF DCE 1.1 for AIX and OS/2," (October 1995) ("Lendenmann")

Lendenmann is a printed publication that was distributed publicly without restriction no later than October 1995. Lendenmann, accordingly, is prior art to the claims of the '181 patent under 35 U.S.C. § 102(b).

4. Exhibit X4 – U.S. Patent No. 6,557,037 to Provino ("Provino").

Provino was filed on May 29, 1998 and issued on April 29, 2003, and is prior art to the '211 patent under 35 U.S.C. § 102(e).

5. Exhibit X5 – Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," November 1987 ("RFC 2131")

RFC 2131 is a printed publication that was publicly distributed no later than March of 1997 and is publicly available at http://www.ietf.org/rfc/rfc2131.txt. RFC 2131, accordingly, is prior art to the '181 patent claims under 35 USC § 102(b).

6. Exhibit X6 – U.S. Patent No. 6,499,108 to Johnson ("Johnson")

Johnson was filed on January 28, 1999 and issue on December 24, 2002, and is prior art to the '181 patent under 35 U.S.C. § 102(e).

7. Exhibit X7 – ITU-T H.323, "Packet-based multimedia communications systems," February 1998 ("H.323")

H.323 is a printed publication that was publicly distributed no later than February of 1998 and is publicly available at http://www.itu.int/rec/T-REC-H.323-199802-S/en. H.323, accordingly, is prior art to the '181 patent claims under 35 U.S.C. § 102(b).

8. Exhibit X8 – ITU-T H.225.0, "Call signaling protocols and media stream packetization for packet-based multimedia communication systems," February 1998 ("H.225.0")

H.225.0 is a printed publication that was publicly distributed no later than February of 1998 and is publicly available at http://www.itu.int/rec/T-REC-H.225.0-199802-S/en. H.225.0, accordingly, is prior art to the '181 patent claims under 35 U.S.C. § 102(b).

9. Exhibit X9 – ITU-T H.235, "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," November 1998 ("H.235")

H.235 is a printed publication that was publicly distributed no later than November of 1998 and is publicly available at http://www.itu.int/rec/T-REC-H.235-199802-S/en. H.235, accordingly, is prior art to the '181 patent claims under 35 U.S.C. § 102(b).

10. Exhibit X10 – ITU-T H.245, "Infrastructure of audiovisual services – Communication procedures," February 1998 ("H.245")

H.245 is a printed publication that was publicly distributed no later than February of 1998 and is publicly available at http://www.ietf.org/rfc/rfc2401.txt. H.245, accordingly, is prior art to the '181 patent claims under 35 U.S.C. § 102(b).

11. Exhibit X11 – Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC 1034")

RFC 1034 is a printed publication that was publicly distributed no later than November of 1987 and is publicly available at http://www.ietf.org/rfc/rfc1034.txt. RFC 1034, accordingly, is prior art to the '181 patent claims under 35 USC § 102(b).

C. Grounds Upon Which Requester Has a Reasonable Likelihood of Prevailing

On September 16, 2011, § 312(a) of title 35, United States Code, was amended to read as follows:

> (a) REEXAMINATION.- Not later than 3 months after the filing of a request for inter partes reexamination under section 311, the Director shall determine whether the information presented in the request shows that there is a reasonable likelihood that the requester would prevail with respect to at least 1 of the claims challenged in the request, with or without consideration of other patents or printed publications. A showing that there is a reasonable likelihood that the requester would prevail with respect to at least 1 of the claims challenged in the request is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office.

See, Pub. Law. 112-29 at §6(c)(3)(A)(i)(I)(aa) and (bb). On September 22, 2011, the Office announced amendments to the rules in Subpart H of 37 CFR governing *inter partes* reexamination. The amended rules specify that a request for reexamination must include "a statement pointing out, based on the cited patents and printed publications, each showing of a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request." *See*, 37 CFR 1.915(b)(3) (revised with effective date of 9/16/2011).

In compliance with Rule 1.915(c)(3), Requester identifies in this request numerous showings that establish a reasonable basis for the Requester prevailing in this proceeding with respect to one or more claims of the '181 patent, including, in particular, that each claim of the '181 patent is anticipated or rendered obvious by the cited patents and/or printed publications. In addition, Requester provides herewith a detailed explanation of why, based on the cited patents and printed publications, the Requester will prevail in its challenge of the claims of the '181 patent in §§ **IV** to **IX**, below. Requester proposes that rejections be imposed based on each of these grounds for the reasons set forth in §§ **IV** to **IX**, below.

1. Claims 1-29 are Anticipated Under 35 U.S.C. § 102(e) by Beser

Beser was not considered by the Office during the original examination of the '181 patent.[1]

Beser teaches systems and methods for establishing secure communication links between two endpoint devices over a network such as the Internet. Beser discloses a variety of services, applications and protocols that may be provided or associated with its systems and methods—including audio, video and multimedia applications. Beser thus describes processes and systems

[1] The '181 patent applicant submitted an IDS describing claim charts that mapped Beser against patents related to the '181. However, Beser itself was never presented to the Examiner in an IDS and there was never an explicit discussion regarding Beser during the prosecution of the '181.

that meet every element of claims 1-29 of the '181 patent, and anticipates these claims under § 102(e).

A claim chart correlating the disclosure of Beser to each of claims 1-29 of the '181 patent is provided as **Exhibit C1**.

A detailed explanation of how Beser anticipates claims 1-29, and which sets forth proposed rejections for these claims, is provided below in **§ IV**. This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

2. Claim 18 Would Have Been Obvious Under 35 U.S.C. § 103 Based on Beser in view of RFC 2401

Beser was not considered by the Office during the original examination of the '181 patent.[2]

Beser teaches systems and methods for establishing secure communication links between two endpoint devices over a network such as the Internet. Beser discloses a variety of services, applications and protocols that may be provided or associated with its systems and methods—including audio, video and multimedia applications. RFC 2401 describes certain security protocols, including authentication protocols, that a person of ordinary skill in the art would have been motivated to combine with Beser. Beser, in view of RFC 2401, thus renders obvious claim 18 of the '181 patent under § 103.

A claim chart correlating the disclosure of Beser, in view RFC 2401, of the '181 patent is provided as **Exhibit C1**.

A detailed explanation of how Beser, in view of RFC 2401, renders obvious claims 1-29, and which sets forth proposed rejections for these claims, is provided below in **§ IV**. This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

3. Claims 1-2, 5-9, 12-17, and 19-22, 24-29 are Anticipated Under 35 U.S.C. § 102(e) by Mattaway

Mattaway was not considered by the Office during the original examination of the '181 patent.

Mattaway describes systems and processes for establishing real-time, point-to-point secure communications between a first and second device. Systems and processes described by Mattaway can evaluate requests and route them to the appropriate secure destination and facilitate voice and/or video communications. Mattaway thus describes systems and processes

[2] The '181 patent applicant submitted an IDS describing claim charts that mapped Beser against patents related to the '181. However, Beser itself was never presented to the Examiner in an IDS and there was never an explicit discussion regarding Beser during the prosecution of the '181.

that meet every element of 1-2, 5-9, 12-17, and 19-22, 24-29 of the '181 patent, and anticipates these claims under § 102(e).

A claim chart correlating the disclosure of Mattaway to each of claims 1-2, 5-9, 12-17, and 19-22, 24-29 of the '181 patent is provided as **Exhibit C2.**

A detailed explanation of how Mattaway anticipates claims 1-2, 5-9, 12-17, and 19-22, 24-29, and which sets forth proposed rejections for these claims, is provided below in **§ V**. This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

4. Claims 3-4, 10-11, 18 and 23 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. § 103 Based on Mattaway in View of Beser

Claims 3-4, 10-11, 18 and 23 depend directly from claim 2.

Mattaway anticipates claim 2 under 35 U.S.C. §102(e).

Beser teaches a system for establishing secure communication links over a network such as the Internet. In addition, Beser discloses a variety of services, applications and protocols that may be provided or associated with its systems – including audio, video and multimedia applications. A person of ordinary skill in the art as of April 2000 would have recognized the benefits of various methods of engaging in secure communications, which benefits were recognized in Mattaway, and would have thus found claims 3-4, 10-11, 18 and 23 obvious based on the teachings of Mattaway in view of Beser.

A claim chart correlating the disclosure of Mattaway in view of Beser to each of claims 3-4, 10-11, 18 and 23 of the '181 patent is provided as **Exhibit C2.**

A detailed explanation of how Mattaway in view of Beser renders obvious claims 3-4, 10-11, 18 and 23, and which sets forth proposed rejections for these claims, is provided below in **§ V**. This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

5. Claims 10-11 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. § 103 Based on Mattaway in View of RFC 2401.

RFC 2401 was considered by the Office during the original examination of the '181 patent. However, the prosecution history of the '181 patent shows that RFC 2401 was cited without any comment or analysis by the applicant. The prosecution history also shows that the Office did not impose any rejections based on RFC 2401 and made no substantive comments concerning this reference. There was no consideration of any reasoning similar to that set forth in the detailed explanation of the RFC 2401 reference and its applicability to the claims of the '181 patent as set forth below, alone or in conjunction with Mattaway. Thus, the RFC 2401 reference considered in a new light establishes a basis for prevailing in this proceeding with respect to at least one claim of the '181 patent.

Mattaway anticipates claim 2 under 35 U.S.C. §102(e).

RFC 2401 defines the IPsec protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes in its "Case 3" VPN implementation a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices will communicate. A person of ordinary skill in the art at the time would have recognized the benefits of various methods of engaging in secure communications, which benefit was also recognized in Mattaway, and would have thus found claims 10-11 obvious based on the teachings of Mattaway in view of RFC 2401.

A claim chart correlating the disclosure of Mattaway in view of RFC 2401 to each of claims 10-11 of the '181 patent is provided as **Exhibit C2.**

A detailed explanation of how Mattaway, in view of RFC 2401, renders obvious claims 10-11, and which sets forth proposed rejections for these claims, is provided below in **§ V.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

6. Claims 1-9, 12-15, and 18-29 are Anticipated Under 35 U.S.C. § 102(b) by Lendenmann

Lendenmann describes a software system that provides a broad set of name resolution and security features for communications via a computer network. Lendenmann thus describes systems that meet every element of 1-9, 12-15, and 18-29 of the '181 patent, and anticipates these claims under § 102(b).

A claim chart correlating the disclosure of Lendenmann to each of claims 1-9, 12-15, and 18-29 of the '181 patent is provided as **Exhibit C3.**

A detailed explanation of how Lendenmann anticipates claims 1-9, 12-15, and 18-29, and which sets forth proposed rejections for these claims, is provided below in **§ VI.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

7. Claims 10-11 and 16-17 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. § 103 Based on Lendenmann in View of Beser.

Claims 10-11 and 16-17 depend directly from claim 2.

Lendenmann anticipates claim 2 under 35 U.S.C. §102(b).

Beser teaches a system for establishing secure communication links over a network such as the Internet. In addition, Beser discloses a variety of services, applications and protocols that may be provided or associated with its systems – including audio, video and multimedia applications. A person of ordinary skill in the art at the time would have recognized the benefits of various methods of engaging in secure communications, which benefits were recognized in

Lendenmann, and would have thus found claims 10-11 and 16-17 obvious based on the teachings of Lendenmann in view of Beser.

A claim chart correlating the disclosure of Lendenmann in view of Beser to each of claims 10-11 and 16-17 of the '181 patent is provided as **Exhibit C3.**

A detailed explanation of how Lendenmann, in view of Beser, renders obvious claims 10-11 and 16-17, and which sets forth proposed rejections for these claims, is provided below in **§ VI**. This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

8. Claims 10-11 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. § 103 Based on Lendenmann in View of RFC 2401.

Claims 10-11 depend directly from claim 2.

Lendenmann anticipates claim 2 under 35 U.S.C. §102(b).

RFC 2401 defines the IPsec protocol, and provides a detailed explanation of how to implement a secure communications links in an IP tunneling model. In particular, RFC 2401 describes in its "Case 3" VPN implementation a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices will communicate. A person of ordinary skill in the art at the time would have recognized the benefits of various methods of engaging in secure communications, which benefit was recognized in Lendenmann, and would have thus found claims 10-11 obvious based on the teachings of Lendenmann in view of RFC 2401.

A claim chart correlating the disclosure of Lendenmann in view of RFC 2401 to each of claims 10-11 of the '181 patent is provided as **Exhibit C3.**

A detailed explanation of how Lendenmann, in view of RFC 2401, renders obvious claims 10-11, and which sets forth proposed rejections for these claims, is provided below in **§ VI**. This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

9. Claims 1-23 and 28-29 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. § 102(e) Based on Provino in View of RFC 2401.

Provino was considered by the Office during the original examination of the '181 patent. A review of the prosecution file history for the '181 patent shows that Provino was cited without detailed comment by the applicant. In addition, there was no rejection based upon or discussion of Provino by the Office during the original examination of the '181 patent. Thus, there was no consideration of any reasoning similar to that set forth below in the detailed explanation of the Provino reference and its applicability to the claims of the '181 patent by the Office during the original examination of the '181 patent. Thus, the prior art effect of Provino on the claims of the

'181 patent viewed in a new light establishes a basis for the prevailing in this proceeding.[3]

Provino describes systems and methods for establishing secure communication links between devices connected to public networks such as the Internet through use of a domain name service system that facilitates the resolution of human readable addresses. The systems and methods described in Provino, in view of RFC 2401, meet every element of claims 1-23 and 28-29 of the '181 patent, and thus render obvious these claims under 35 U.S.C. § 103.

A claim chart correlating the disclosure of Provino to each of claims 1-23 and 28-29 of the '181 patent is provided as **Exhibit C4**.

A detailed explanation of how Provino, in view of RFC 2401, renders obvious claims 1-23 and 28-29, and which sets forth proposed rejections for these claims, is provided below in **§ VII.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

10. Claims 24-27 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. §103 Based on Provino taken in view of H.323.

A claim chart correlating the disclosure of Provino in view of H.323 to each of claims 24-27 of the '181 patent is provided as **Exhibit C4**.

Provino was considered by the Office during the original examination of the '181 patent. A review of the prosecution file history for the '181 patent shows that Provino was cited without detailed comment by the applicant. In addition, there was no rejection based upon or discussion of Provino by the Office during the original examination of the '181 patent. Thus, there was no consideration of any reasoning similar to that set forth below in the detailed explanation of the Provino reference and its applicability to the claims of the '181 patent by the Office during the original examination of the '181 patent. Thus, the prior art effect of Provino on the claims of the '181 patent viewed in a new light establishes a basis for the prevailing in this proceeding.

Provino describes systems and methods for establishing secure communication links between devices connected to public networks such as the Internet through use of a domain name service system that facilitates the resolution of human readable addresses. A person of ordinary skill in the art would have recognized the value of adding the methods describing registering secure and unsecure domain names with that of H.323 given its global appeal.

The Telecommunication Sector of the International Telecommunications Union (ITU-T) developed a series of recommendations that comprise the H.323 standard, which provides for

[3] *See* MPEP § 2242, "a substantial new question of patentability may be based solely on old art where the old art is being presented/viewed in a new light, or in a different way, as compared with its use in the earlier examination(s)." *See also* 35 USC § 303(c), "[t]he existence of a substantial new question of patentability is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office." Requester notes that the MPEP has not been revised in connection with the law and rule changes noted above.

secure multimedia communications in packet-based networks. The H.323 standard includes the teaching and disclosure of H.225.0, "core message definitions," H.235, "security framework," and H.245, "media channel control." These recommendations are incorporated by reference because they are specifically referenced and described as disclosing particular features of the H.323 standard.

A detailed explanation of how Provino, in view of H.323 renders obvious claims 24-27, and which sets forth proposed rejections for these claims, is provided below in **§ VII.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

11. Claims 1-29 are Anticipated Under 35 U.S.C. § 102(b) Based on H.323

H.323 was not considered during the prosecution of the H.323 patent.[4]

A claim chart correlating the disclosure of H.323 to each of claims 1-29 of the '181 patent is provided as **Exhibit C5**.

The Telecommunication Sector of the International Telecommunications Union (ITU-T) developed a series of recommendations that comprise the H.323 standard, which provides for secure multimedia communications in packet-based networks. The H.323 standard includes the teaching and disclosure of H.225.0, "core message definitions," H.235, "security framework," and H.245, "media channel control." These recommendations are incorporated by reference because they are specifically referenced and described as disclosing particular features of the H.323 standard.

A detailed explanation of how H.323 anticipates claims 1-29, and which sets forth proposed rejections for these claims, is provided below in **§ VIII.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

12. Claims 1-29 Would Have Been Obvious to A Person of Ordinary Skill Under 35 U.S.C. § 103 Based on H.323 in view of H.225, H.235, and H.245.

H.323 was not considered during the prosecution of the H.323 patent.[5]

A claim chart correlating the disclosure of H.323 to each of claims 1-29 of the '181 patent is provided as **Exhibit C5**.

[4] The '181 patent applicant submitted an IDS describing claim charts that mapped H.323 against patents related to the '181. However, H.323 itself was never presented to the Examiner on an IDS and there was never explicit discussions regarding H.323 during the prosecution of the '181.

[5] The '181 patent applicant submitted an IDS describing claim charts that mapped H.323 against patents related to the '181. However, H.323 itself was never presented to the Examiner on an IDS and there was never explicit discussions regarding H.323 during the prosecution of the '181.

The Telecommunication Sector of the International Telecommunications Union (ITU-T) developed a series of recommendations that comprise the H.323 standard, which provides for secure multimedia communications in packet-based networks. The H.323 standard includes the teaching and disclosure of H.225.0, "core message definitions," H.235, "security framework," and H.245, "media channel control." As explained above in **No. 11**, and in **§ VIII** below, H.323 anticipates the '181 patent because the H.323 standard incorporates the teaching and disclosures of the H.225, H.235, H.245 series of recommendations. To the extent those series of recommendations are not incorporated by reference, and for the same reasons expressly described in **§ VIII (A)(1)-A(29)** with regard to anticipation, it would have been obvious to one of ordinary skill to combine the teachings of the H.323 standard with the H.225, H.235, and H.245 series of recommendations as there is an express motivation to combine those various documents because they are specifically referenced and described in the H.323 as disclosing particular features of H.323 and there are indications in H.323 that they be used together as elements of the H.323 standard.

A detailed explanation of how H.323 renders claims 1-29 obvious in view of H.225, H.235, and H.245, and which sets forth proposed rejections for these claims, is provided below in **§ VIII.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

13. Claims 1-16 and 18-29 Would Have Been Obvious to a Person of Ordinary Skill Under 35 U.S.C. § 103 based on Johnson in view of RFC 2131, RFC 1034 and RFC 2401.

A claim chart correlating the disclosure of Johnson in view of RFC 2131, RFC 1034 and RFC 2401 to each of claims 1-16 and 18-29 of the '181 patent is provided as **Exhibit C6**.

Johnson discloses systems and methods for transferring messages securely over a computer network. The disclosed invention has utility in applications involving person-to-person communications over the Internet where a secure communication link is desired. It would have been obvious to a person of ordinary skill in the art to combine the teachings of Johnson with the RFC 2131 and RFC 1034—which describe low-level details for implementing communications over the Internet, together with RFC 2401, which describes methods for securing such communications.

A detailed explanation of how Johnson, in view of RFC 2131, RFC 1034, and RFC 2401 renders obvious claims 1-16 and 18-29, and which sets forth proposed rejections for these claims, is provided below in **§ IX.** This explanation establishes a reasonable likelihood that Requester will prevail with respect to at least one claim of the '181 patent.

III. Previous Findings and Observations Concerning Terms in Claims 1-29 of the '181 Patent

In reexamination proceedings before the Office, claims must be given their broadest reasonable construction. *See* In re Yamamoto, 740 F.2d 1569, 1571 (Fed. Cir. 1984); In re Trans Texas Holdings Corp., 498 F.3d 1290, 1297 (Fed. Cir. 2007).

The '180 patent, which is a parent to the '181 patent, has been the subject of two prior reexaminations. It should be noted that during the first reexamination, Control No. 95/001,270, the Patent Owner distinguished the methods and systems claimed in the '181 patent by asserting that the claim terms "secure domain name" and "secure domain name service" had particular meanings that were not equivalent to conventional meanings associated with the terms domain name and domain name service. In particular, the '180 patentee stated:

> The '180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a convention[al] domain name server using a secure domain name will result in a return message indicating that the URL is unknown ('180 patent at 51:25-35) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name ('180 patent at 51:25-35).[6]

The '181 patent owner also has taken a position as to what the terms "secure domain name" and "secure domain name service" as used in the '181 patent claims may encompass. For example, the '181 patent owner stated:

> [T]he Applicant submits that a "secure name" is a name associated with a network address associated of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device. The claimed "secure name" includes, but is not limited to, a secure domain name. For example, a "secure name" can be a secure non-standard domain name, such as a secure non-standard top-level domain name (*e.g.*, .scom) or a telephone number.[7]

Thus, the file history of the '181 patent and the reexamination records of the related '180 patent contain representations made by the '181 patent owner that the Patent Office may properly consider in evaluating the broadest reasonable construction that can be given to the claims of the '181 patent.

[6] Reexamination Control No. 95/001,270, Action Closing Prosecution at 13-14 (Jun. 16, 2010)

[7] File History of '181, Applicant Remarks/Arguments at 9 (Oct. 8, 2010)

IV. DETAILED EXPLANATION OF MANNER OF APPLYING BESER TO CLAIMS 1-29 AND PROPOSED REJECTIONS BASED ON GROUND NOS. 1-2.

Exhibit C1 correlates each of claims 1-29 of the '181 patent with the section of the present request that sets out the detailed basis for anticipation of the claim, along with an identification of the relevant portions of Beser. Requester notes that any emphasis indicated in quotations or other citations (e.g., as shown in bold faced text) has been added and is not original to the references cited in this section, unless otherwise noted.

A. Ground No. 1: Claims 1-29 are Unpatentable under 35 USC § 102(e) as Being Anticipated by Beser

Beser describes methods and systems for initiating a secured communication link—via "tunneling"—between networked devices over a public network, such as the Internet. Specifically, Beser explains that its method involves "negotiating private addresses, such as a private Internet Address, for the ends of the tunneling association." *See* Beser, ABSTRACT. Beser further explains that:

> The negotiation is performed on a public network, such as the Internet, through a trusted-third party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network. Beser, ABSTRACT.

Beser explains that its methods involve a first and second network device, and a "trusted-third-party network device." According to Beser, the first and second network device "may be modified routers or modified gateways." Beser at 4:7-11. Beser further explains that in an exemplary preferred embodiment, the first or second network devices are an "edge router," which Beser explains "routes data packets between one or more networks such as a backbone network (e.g., a public network 12) and Local Area Networks (e.g., private network 20)." Beser at 4:19-24. An edge router is a computer, as it has a CPU, memory and storage.

Beser further explains that "the data network also includes network devices (24, 26) that are originating and terminating ends of data flow." Beser at 4:43-44. Beser indicates that these devices can include telephony and multimedia devices, and further, that:

> Multimedia devices include Web-TV sets and decoders, interactive video-game players, or **personal computers running multimedia applications**. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:47-50.

The data that is to be transmitted through the secure communication tunnels constructed by the Beser systems and methods can include web pages (e.g., delivered to WebTV devices or decoders or personal computers), video, or voice. Beser at 4:47-50.

Beser thus describes methods and systems for establishing a secure communication link between two devices across a public network such as the Internet.

1. Claim 1

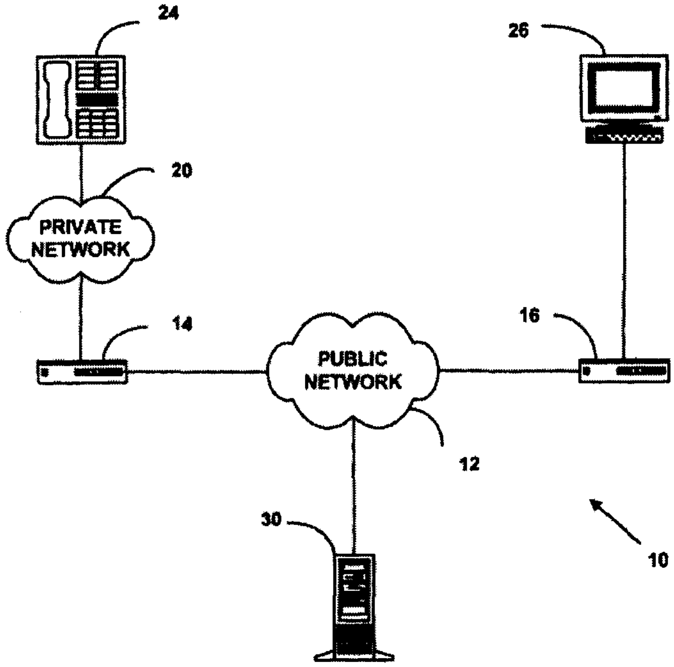
Claim 1 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising":

(a) receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and

(b) sending a message over a secure communication link from the first device to the second device.

The preamble of claim 1 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name . . . ." Beser describes programs, processes, methods systems and apparatus that include, but are not limited to, computer hardware or software. Beser at 25:42-26. In particular, Beser teaches—as shown below in Figure 1—a first network device (14), a second network device (16), two end-point devices (24, 26), which may be Voice Over Internet Protocol ("VoIP") phones, and a trusted third party device (30):

FIG. 1



The first network device (14) and second network device (16) may be modified routers or gateways, and the trusted-third-party device 30 may be "a back-end service, a domain name server or the owner/manager of database or directory services." Beser at 4:5-11. Beser further explains that end-point devices (24, 26) are "originating and terminating ends of data flow." Beser at 4:43-44. Beser indicates that these end-point devices can include telephony and multimedia devices. For example, Beser explains that:

> Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices.

Beser at 4:47-50.

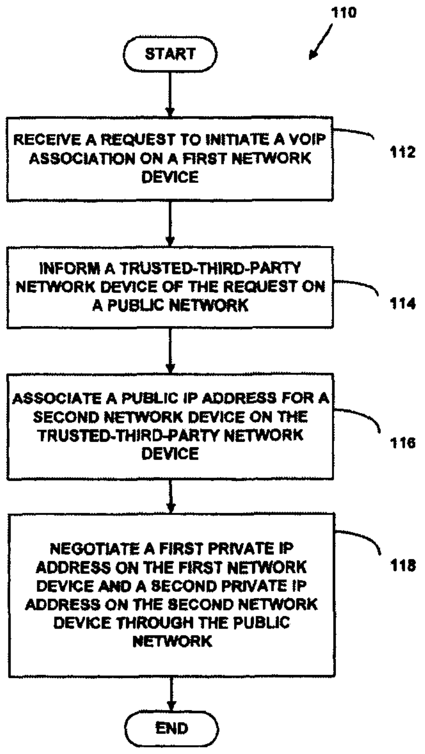
First and second network devices (14, 16) and end-point devices (24, 26) have associated therewith both secure and unsecure names. For example, end-point devices (24, 26) each have an secure name that comprises a "unique identifier" that is registered with the trusted-third-party device (30). Beser at 11:28-32 ("The second network device 16 is associated with the terminating telephony device 26. This association of the public IP address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30."). The unique identifier may be "any of a dial-up number, an electronic mail address, or a domain name." Beser at 10:37-41.

The systems and methods described in Beser show that the secure name is associated with a "private IP address." The private IP addresses are, for example, associated with each originating and terminating ends of a tunneling association. Private IP addresses are themselves secure in that they are not intended to be known by external devices (or users) and must be negotiated for through the systems and methods disclosed in Beser. The unique identifier is a secure name because apart from being secure itself, Beser at 11:22-24 ("The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12)," it is designed to protect the integrity of the private IP address and ensure the anonymity of the terminating devices. For example:

> The IP 58 packets of the negotiation step 118 will only have source 88 or destination 90 address fields containing the IP 58 addresses of the first 14, second 16, or trusted-third-party 30 network device. In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. **The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26).** Beser at 12:9-19.

The initiation of a secure communication link and negotiation of private IP addresses is represented in, for example, Figure 5. The anonymity and discrete measures disclosed in Beser facilitate a secure communication process. In addition, Beser teaches that one could use IPSEC in order to enhance the secure communications described in Beser. Beser at 1:54-56 ("[T]he send may encrypt the information inside the IP packets before transmission, e.g., with IP Security.").

FIG. 5


110
START
RECEIVE A REQUEST TO INITIATE A VOIP ASSOCIATION ON A FIRST NETWORK DEVICE
112
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
114
ASSOCIATE A PUBLIC IP ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
116
NEGOTIATE A FIRST PRIVATE IP ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE IP ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
118
END

Beser shows that an "unsecure name" is also associated with a "first device." In particular, each network device has associated with it a "public IP address." The "public IP address" is associated with the unique identifier and the first network device 24. As each end-point device have associated therewith a unique identifier, the public IP address—the unsecure name—is thus associated with each end-point device. Or, as explained in Beser :

> A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at Step 116. The second network device 16 is associated with the terminating telephony device 26. This association of the public IP 58 address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30. Beser at 11:25-32.

Thus, Beser discloses "a non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name."

Step (a) of Claim 1 specifies: "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and"

Beser teaches that private IP addresses are assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26) and are negotiated via a negotiation process initiated through the trusted-third-party device 30. Beser at 11:59-62 ("At

Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12.") The negotiation and discovery of the private IP addresses are facilitated by the disclosure of the "unique identifier" associated with the terminating devices. Beser at 11:26-37. After negotiation, the private IP addresses are recorded at the trusted-third-party-device:

> Once negotiated, on the first network device 14 is recorded the first private IP 58 address for the originating telephony device 24, and on the second network device 16 is recorded the second private IP 58 address for the terminating telephony device 26. These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective ends of the VoIP association by methods known to those skilled in the art.

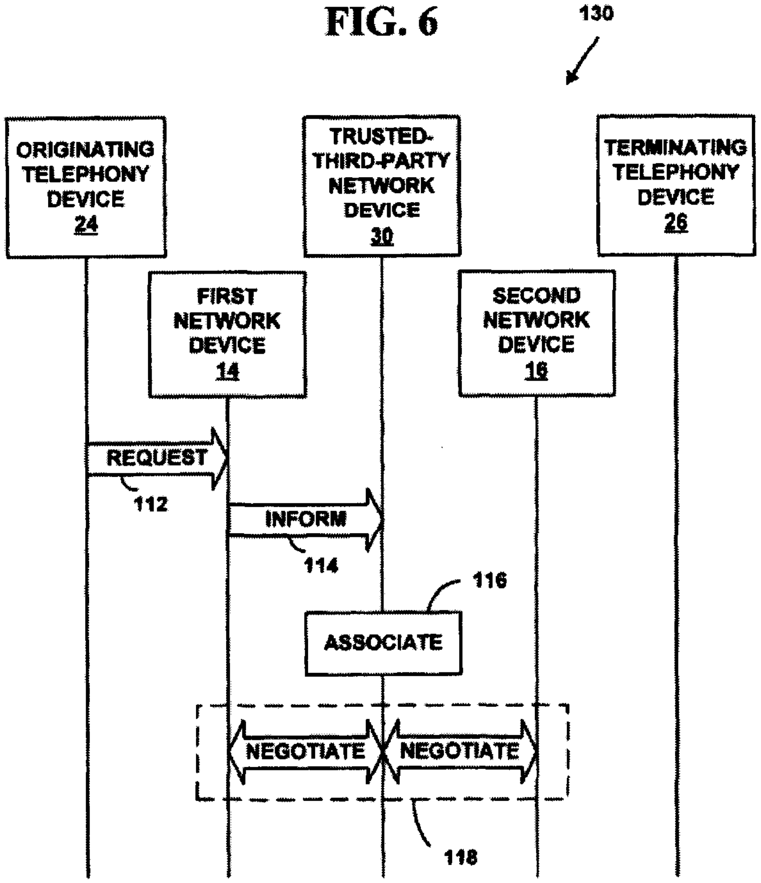
Beser at 12:28-36. Beser shows that security measures can be utilized which result in receiving, at a network address corresponding to the secure device, a message from a second device of the desire to securely communicate. For example, tunneling—a method of communicating securely—is taught in Beser :

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network.

Beser at 2:6-12. The communications link described in Beser is secure because the "tunneling association hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network," thus preventing public disclosure or interception by hackers. Beser at 2:35-40. Further, under the broadest reasonable interpretation of this claim element, encryption of the communication link is not required. Nevertheless, Beser describes that as another method of securely communicating, "the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec")." Beser at 1:54-56. It was known by one of ordinary skill in the art at the time of the filing of Beser that IPSec security required negotiating Security Associations before secure communications begin, which required messages to be exchanged, including a message requesting the desire to communicate securely.

The request and negotiation process described above between the end-point devices in order to establish a secure communications link between the end-point devices is represented diagrammatically in Figure 6:

FIG. 6



The trusted-third-party network device 30, which can be domain name server, recognizes that the unique identifier received from the querying device requires special processing, and it alters its normal operation by, instead of resolving the domain name, for example, establishing "a virtual tunneling association between the originating end and the terminating end of the tunneling association without revealing the identities of both ends of the tunneling association on the public network," Beser at 8:15-20. The trusted-third-party network device 30, i.e., the secure name server, protects the unique identifier from discovery on the Internet by, e.g., encrypting and authenticating communications to/from the device making the query. Beser at 11:20-25.

Thus, Beser discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

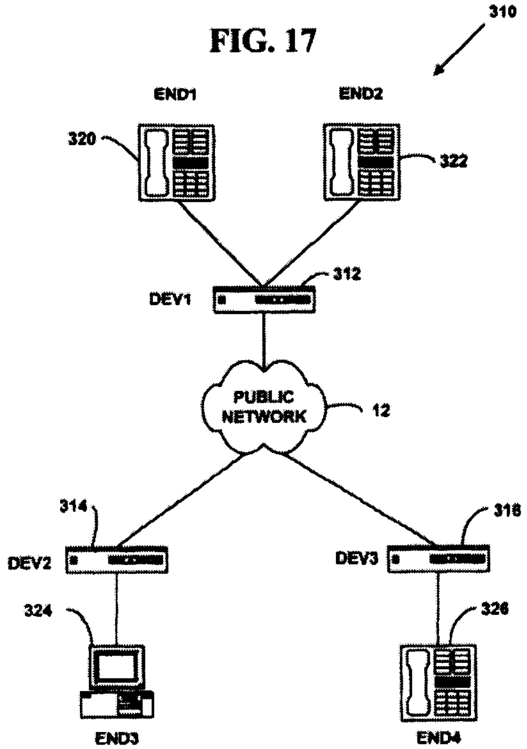
Step (b) of claim 1 specifies: "sending a message over a secure communication link from the first device to the second device."

Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Beser also discloses and describes methods that facilitate establishment of a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Beser, for example, discloses, following the negotiation described above, that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association."

Thus, Beser discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 1 of the '181 patent under 35 U.S.C. § 102(e).

2. Claim 2

Independent claim 2 is directed to "[a] method of using a first device to communicate with a second device having a secure name, the method comprising:

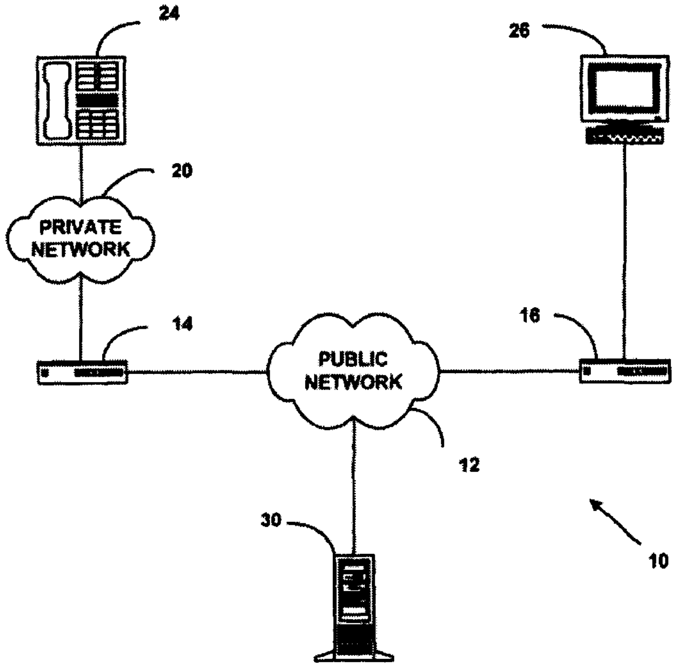
(a) from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;

(b) at the first device, receiving a message containing the network address associated with the secure name of the second device; and

(c) from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

The preamble of claim 2 specifies "[a] method of using a first device to communicate with a second device having a secure name . . . ." Beser describes programs, processes, methods systems and apparatus that include, but are not limited to, computer hardware or software. Beser at 25:42-26. In particular, Beser teaches—as shown below in Figure 1—a first network device (14), a second network device (16), two end-point devices (24, 26), which may be Voice Over Internet Protocol ("VoIP") phones, and a trusted third party device (30):

FIG. 1



The first network device (14) and second network device (16) may be modified routers or gateways, and the trusted-third-party device 30 may be "a back-end service, a domain name server or the owner/manager of database or directory services." Beser at 4:5-11. Beser further explains that end-point devices (24, 26) are "originating and terminating ends of data flow." Beser at 4:43-44. Beser indicates that these end-point devices can include telephony and multimedia devices. For example, Beser explains that:

> Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:47-50.

Beser also teaches that both secure and unsecure names are associated with the first and second network devices (14, 16) and end-point devices (24, 26). For example, Beser teaches that end-point devices (24, 26) each have a secure name that comprises a "unique identifier" that is registered with the trusted-third-party device (30). Beser at 11:28-32 ("The second network device 16 is associated with the terminating telephony device 26. This association of the public IP address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30."). The unique identifier may be "any of a dial-up number, an electronic mail address, or a domain name." Beser at 10:37-41.

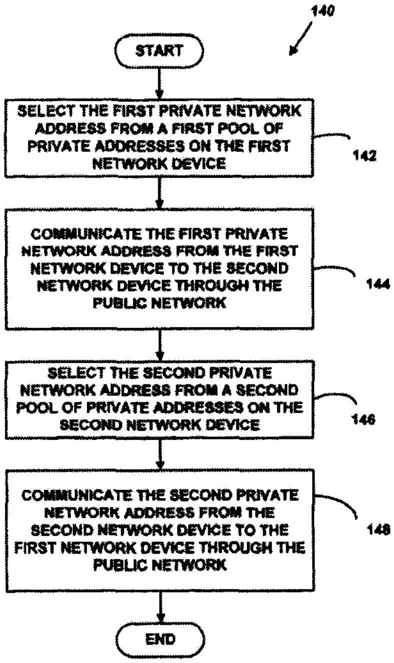
Thus, Beser discloses "[a] method of using a first device to communicate with a second device having a secure name."

Step (a) of claim 2 further specifies: "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Beser teaches that private IP addresses are assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26) and are negotiated via a negotiation process initiated through the trusted-third-party device 30. Beser at 11:59-62 ("At Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12."). Beser discloses that the trusted-third-party device (3) is a secure name service. Beser at 4:5-11 (The trusted-third-party 30 may be a back-end service, a domain name server, or the owner/manager of database or directory services.")

In particular, the negotiation process in Beser, as depicted in Figure 7 below, commences by "receiving a request to initiate the VoIP association on a first network device 14 at Step 112. The first network device 14 is associated with the origination telephony device 24, and the request includes a unique identifier for the terminating telephony device 26." Beser at 10:2-6. Further, "[a]t Step 114, a trusted-third-party network device 30 is informed of the request on the public network 12," Beser at 11:9-10, and at Step 116, "a public IP 48 address for a second network device 16 is associated with the unique identifier [supplied by network device 14] for the terminating telephony device 26." Beser at 11:25-29.

FIG. 7


140
START
SELECT THE FIRST PRIVATE NETWORK ADDRESS FROM A FIRST POOL OF PRIVATE ADDRESSES ON THE FIRST NETWORK DEVICE
142
COMMUNICATE THE FIRST PRIVATE NETWORK ADDRESS FROM THE FIRST NETWORK DEVICE TO THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
144
SELECT THE SECOND PRIVATE NETWORK ADDRESS FROM A SECOND POOL OF PRIVATE ADDRESSES ON THE SECOND NETWORK DEVICE
146
COMMUNICATE THE SECOND PRIVATE NETWORK ADDRESS FROM THE SECOND NETWORK DEVICE TO THE FIRST NETWORK DEVICE THROUGH THE PUBLIC NETWORK
148
END

Thus, Beser shows the step of "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Step (b) of claim 2 further specifies: "at the first device, receiving a message containing the network address associated with the secure name of the second device; and"

Following the negotiation, the first network device (14)—the requesting device—has obtained "the following network addresses: the public network address of the second network device 16, and the private network addresses assigned to the originating 24 and terminating 26 ends of the tunneling association." Beser at 21:38-43. Thus, Beser shows the step of "at the first device, receiving a message containing the network address associated with the secure name of the second device."

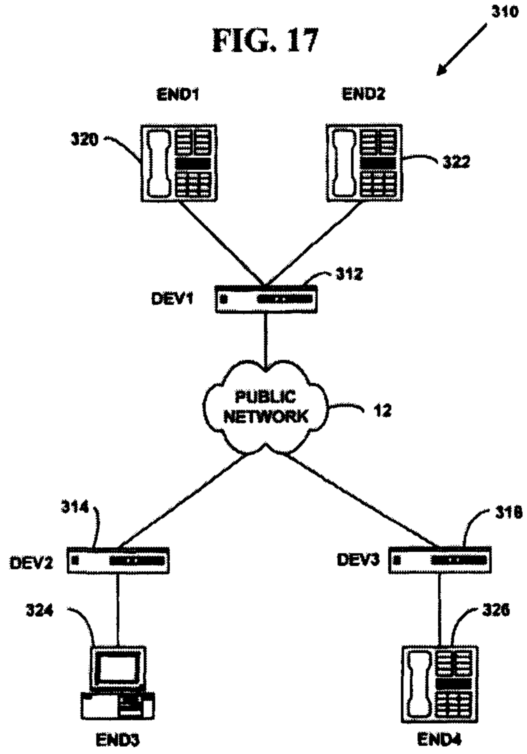
Step (c) of claim 2 further specifies: "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Beser also teaches methods which facilitate establishment of a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Following the negotiation described above, Beser discloses that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association." Thus, Beser discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 2 of the '181 patent under 35 U.S.C. § 102(e).

3. Claim 3

Claim 3 depends from claim 2, and specifies "wherein the secure name of the second device is a secure domain name.

The "secure name," i.e., the "unique identifier," can be a secure domain name. Beser at 10:38-41 ("In another exemplary preferred embodiment of the present invention, the unique identifier is any of a dial-up number, an electronic mail address, or a **domain name**."). The secure domain name of Beser (e.g., the E.164 telephone number, e-mail address, or domain name) is associated with each terminating device and is used in Beser to facilitate a secure communication another terminating device. Beser thus teaches that a "secure domain name" can include both standard and non-standard domain names.

Accordingly, Beser anticipates claim 3 of the '181 patent under 35 U.S.C. § 102(e).

4. Claim 4

Claim 4 depends from claim 2, and specifies "wherein the secure name indicates security."

The unique identifier disclosed in Beser is recognized by the trusted-third-party device as being secure and therefore implements protocols in order to obfuscate it from discovery by untrusted parties:

> For each transfer of a packet from the first network device 14 to the trusted-third-party network device 30, the first network device 14 constructs an IP 58 packet. . . . **The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12**. Beser at 11:13-25 (emphasis added).

Accordingly, Beser anticipates claim 4 of the '181 patent under 35 U.S.C. § 102(e).

5. Claim 5

Claim 5 of the '181 patent depends from claim 2, and specifies "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form."

Beser shows that the negotiation process is performed in order to protect against hackers obtaining the identities of the originating and terminating telephony devices:

> The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90 address fields of the IP 58 packets that comprise the negotiation. . . . In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26). Beser at 12:6-19.

Additionally, Beser teaches that when anonymity is required, encryption can be used:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. Beser at 2:6-12.

Beser additionally shows that "the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec")." Beser at 1:54-56.

Accordingly, Beser anticipates claim 5 of the '181 patent under 35 U.S.C. § 102(e).

6. Claim 6

Claim 6 depends from claim 5, and specifies that the step of "further including decrypting the message."

It would have been inherent in Beser to "decrypt" the very information that it recommends encrypting.

Accordingly, Beser anticipates claim 6 of the '181 patent under 35 U.S.C. § 102(e).

7. Claim 7

Claim 7 of the '181 patent depends from claim 2, and specifies "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed."

Beser teaches that first and second network devices (14, 16) and endpoint devices (24, 26), include any device that can interact on network system 10 based on standards proposed including, among others, the IETF:

> Network devices and routers for preferred embodiments of the present invention include network devices that can interact with network system 10 based on standards proposed by the Institute of Electrical and Electronic Engineers ("IEEE"), International Telecommunications Union-Telecommunication Standardization Sector ("ITU"), Internet Engineering Task Force ("IETF"), or Wireless Application Protocol ("WAP") Forum. However, network devices based on other standards could also be used. Beser at 4:55-63.

Thus, the standards-based system and methods disclosed in Beser would be able to implement a far-less obtrusive non-secure communications link, if necessary.

Accordingly, Beser anticipates claim 7 of the '181 patent under 35 U.S.C. § 102(e).

8. Claim 8

Claim 8 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

Following the negotiation, the first network device (14)—the requesting device—has obtained "the following network addresses: the public network address of the second network device 16, and the private network addresses assigned to the originating 24 and terminating 26 ends of the tunneling association." Beser at 21:38-43. Thus, Beser shows the step of "at the first device, receiving a message containing the network address associated with the secure name of the second device."

Accordingly, Beser anticipates claim 8 of the '181 patent under 35 U.S.C. § 102(e).

9. Claim 9

Claim 9 depends from claim 2 and specifies that "further including automatically initiating the secure communication link after it is enabled."

The security methods described in Beser, including the establishment of the secure communication link via a tunneling association, are disclosed without reference to user interaction and therefore would be established automatically.

Accordingly, Beser anticipates claim 9 of the '181 patent under 35 U.S.C. § 102(e).

10. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

Beser shows that one of the security measures that can be performed by the disclosed methods "is that of initiating and maintaining a virtual tunnel." Beser at 6:58-59. Beser emphasizes the importance of protecting the negotiation process in order to protect from hackers the identities of the originating and terminating telephony devices:

> The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90 address fields of the IP 58 packets that comprise the negotiation. . . . In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26). Beser at 12:6-19.

Additionally, Beser teaches that when anonymity is required, encryption can be used:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. Beser at 2:6-12.

Accordingly, Beser anticipates claim 10 of the '181 patent under 35 U.S.C. § 102(e).

11. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

Beser shows that one of the security measures that can be performed by the disclosed methods "is that of initiating and maintaining a virtual tunnel." Beser at 6:58-59. Beser emphasizes the importance of protecting the negotiation process in order to protect hackers from obtaining the identities of the originating and terminating telephony devices:

> The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90 address fields of the IP 58 packets that comprise the negotiation. . . . In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26). Beser at 12:6-19.

Additionally, Beser teaches that when anonymity is required, encryption can be used:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. Beser at 2:6-12.

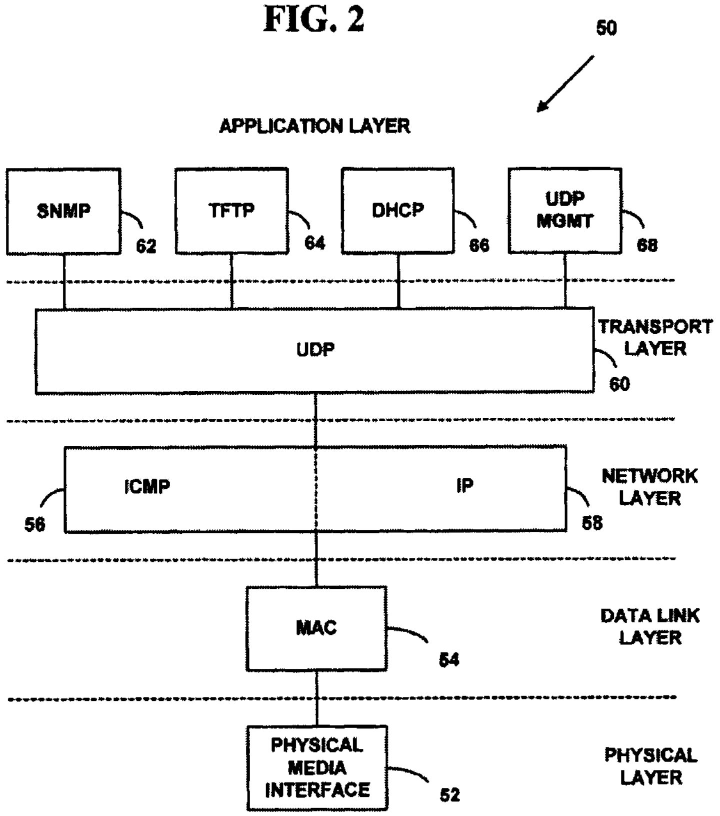
Accordingly, Beser anticipates claim 11 of the '181 patent under 35 U.S.C. § 102(e).

12. Claim 12

Claim 12 depends from claim 2 and specifies "wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols."

As depicted in Figure 2, Beser discloses a plurality of protocols for networked devices in its described methods and systems:

FIG. 2



See also Beser at 5:49–7:60 (describing the protocols depicted in Figure 2).

Accordingly, Beser anticipates claim 12 of the '181 patent under 35 U.S.C. § 102(e).

13. Claim 13

Claim 13 depends from claim 2 and specifies "wherein the receiving and sending of messages through the secure communication link includes multiple sessions."

Beser shows that the disclosed methods and systems can facilitate secure communications between, for example, telephony devices, and other multimedia, which would inherently require multiple sessions:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Accordingly, Beser anticipates claim 13 of the '181 patent under 35 U.S.C. § 102(e).

14. Claim 14

Claim 14 depends from claim 2 and specifies "further including supporting a plurality of services over the secure communication link."

Beser discloses a plurality of services and multimedia applications that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

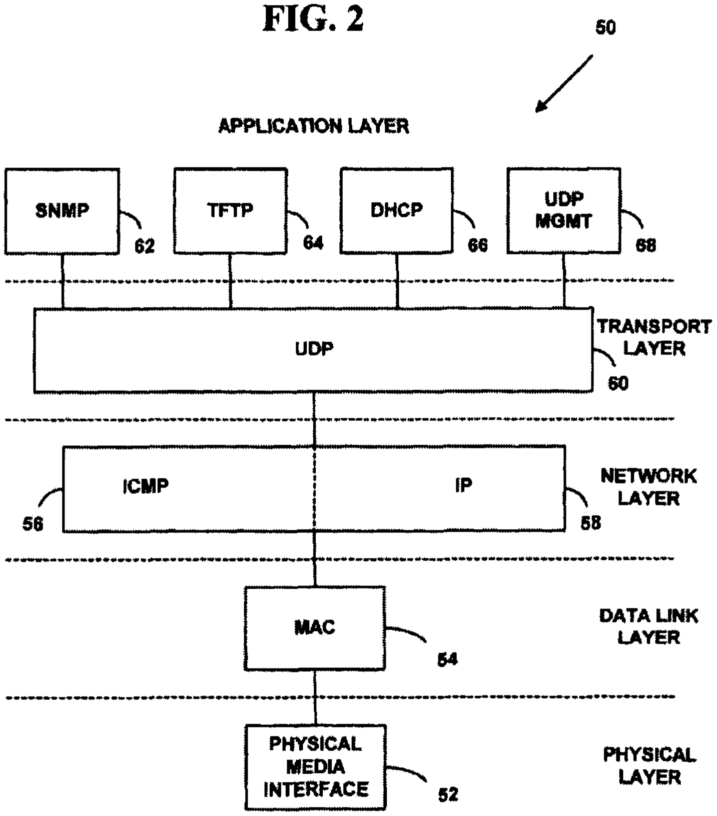
Accordingly, Beser anticipates claim 14 of the '181 patent under 35 U.S.C. § 102(e).

15. Claim 15

Claim 15 depends from claim 14 and specifies "wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof."

As depicted in Figure 2, Beser discloses the protocol stack for networked devices in its described methods and systems:

FIG. 2



See also Beser at 5:49–7:60 (describing the protocols depicted in Figure 2).

Beser also discloses a plurality of services and multimedia applications that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

As it is inherent in the disclosure of Beser, multimedia applications would necessarily need to facilitate multiple sessions.

Accordingly, Beser anticipates claim 15 of the '181 patent under 35 U.S.C. § 102(e).

16. Claim 16

Claim 16 depends from claim 15 and specifies "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof."

Beser also discloses a plurality of services and multimedia applications that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Accordingly, Beser anticipates claim 16 of the '181 patent under 35 U.S.C. § 102(e).

17. Claim 17

Claim 17 depends from claim 15 and specifies "wherein the plurality of services comprises audio, video or a combination thereof."

Beser also discloses a plurality of services and multimedia applications that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Accordingly, Beser anticipates claim 17 of the '181 patent under 35 U.S.C. § 102(e).

18. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

Beser specifies that authentication and encryption should be used to establish IP tunnels. *See, e.g.,* Beser at 11:22-24 ("the IP 58 packets may require encryption and authentication to ensure that the unique identifier cannot be read on the public network.")

Accordingly, Beser anticipates claim 18 of the '181 patent under 35 U.S.C. § 102(e).

19. Claim 19

Claim 19 depends from claim 2 and specifies "wherein the first device is a computer, and the steps are performed on the computer."

Beser also discloses a plurality of multimedia devices, including personal computers, that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or **personal computers** running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or **personal computers** running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54 (emphasis added).

Accordingly, Beser anticipates claim 19 of the '181 patent under 35 U.S.C. § 102(e).

20. Claim 20

Claim 20 depends from claim 2 and specifies "wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network."

Beser also discloses a plurality of multimedia devices, including personal computers, that are able to utilize the disclosed secure communication links. For example:

> **The data network also includes network devices (24, 26) that are originating and terminating ends of data flow**. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or **personal computers** running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or **personal computers** running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54 (emphasis added).

Accordingly, Beser anticipates claim 20 of the '181 patent under 35 U.S.C. § 102(e).

21. Claim 21

Claim 21 depends from claim 2 and specifies "further including providing an unsecured name associated with the device."

Beser shows that an "unsecure name" is also associated with a "first device." In particular, each network device has associated with it a "public IP address." The "public IP address" is associated with both the unique identifier and the first network device 24. As each end-point device have associated therewith a unique identifier, the public IP address—the unsecure name—is thus associated with each end-point device. Or, as explained in Beser :

> A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at Step 116. The second network device 16 is associated with the terminating telephony device 26. This association of the public IP 58 address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30. Beser at 11:25-32.

Accordingly, Beser anticipates claim 21 of the '181 patent under 35 U.S.C. § 102(e).

22. Claim 22

Claim 22 depends from claim 2 and specifies "wherein the secure name is registered prior to the step of sending a message to a secure name service."

Beser discloses, for example, an embodiment in which the unique identifier, i.e., secure name, is an E.164 telephone number. An E.164 telephone number, Beser explains, "is an ITU recommendation for the assignment of telephone numbers on a world wide basis." Beser at 10:45-48. To that end, Beser shows that "the trusted-third-party network device 30 may be a directory service, owned and operated by a telephone company **that retains a list of E.164 numbers of its subscribers**."

Accordingly, Beser anticipates claim 22 of the '181 patent under 35 U.S.C. § 102(e).

23. Claim 23

Claim 23 depends from claim 2 and specifies "wherein the secure name of the second device is a secure, non-standard domain name."

The "secure name," i.e., the "unique identifier," can be a secure domain name. Beser at 10:38-41 ("In another exemplary preferred embodiment of the present invention, the unique identifier is any of a dial-up number, an electronic mail address, or a domain name."). The non-standard secure domain name of Beser (e.g., the E.164 telephone number or e-mail address) is associated with each terminating device and is used in Beser to facilitate a secure communication with another terminating device.

Accordingly, Beser anticipates claim 23 of the '181 patent under 35 U.S.C. § 102(e).

24. Claim 24

Independent claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network, the method comprising:

(a) at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;

(b) receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and

(c) sending a message securely from the first device to the second device."

The preamble of claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network." As described in Beser, at 3:1-10:

> [T]he method and system of the present invention may provide for the initiation of a Voice-overInternet-Protocol association between an originating telephony device and a terminating telephony device. The method and system described herein may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication without an increased computational burden.

Thus, Beser discloses "[a] method of using a first device to securely communicate with a second device over a communication network."

Step (a) of claim 24 further specifies: "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

Beser discloses, for example, an embodiment in which the unique identifier, i.e., secure name, is an E.164 telephone number. An E.164 telephone number, Beser explains, "is an ITU recommendation for the assignment of telephone numbers on a world wide basis." Beser at 10:45-48. To that end, Beser shows that "the trusted-third-party network device 30 may be a directory service, owned and operated by a telephone company **that retains a list of E.164 numbers of its subscribers**." Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name.

Step (b) of claim 24 further specifies: "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and."

Beser teaches that private IP addresses are assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26) and are negotiated via negotiation process initiated through the trusted-third-party device 30. Beser at 11:59-62 ("At Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12.") The negotiation and discovery of the private IP addresses are facilitated by the disclosure of the "unique identifier" associated with the terminating devices. Beser at 11:26-37. After negotiation, the private IP addresses are recorded at the trusted-third-party-device:

> Once negotiated, on the first network device 14 is recorded the first private IP 58 address for the originating telephony device 24, and on the second network device 16 is recorded the second private IP 58 address for the terminating telephony device 26. These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective ends of the VoIP association by methods known to those skilled in the art.

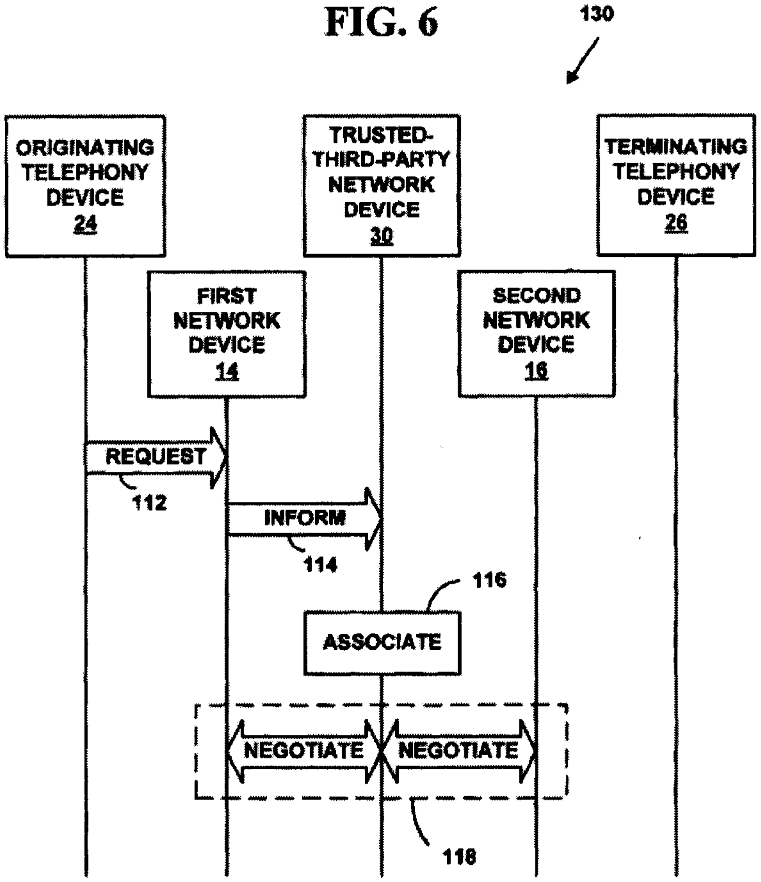
Beser at 12:28-36. Beser shows that security measures can be utilized which result in receiving, at a network address corresponding to the secure device, a message from a second device of the desire to securely communicate. For example, tunneling—a method of communicating securely—is taught in Beser:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network.

Beser at 2:6-12. The communications link described in Beser is secure because the "tunneling association hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network," thus preventing public disclosure or interception by hackers. Beser at 2:35-40. Further, under the broadest reasonable interpretation of this claim element, encryption of the communication link is not required. Nevertheless, Beser describes that as another method of securely communicating, "the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec")." Beser at 1:54-56. It was known by one of ordinary skill in the art at the time of the filing of Beser that IPSec security required negotiating Security Associations before secure communications begin, which required messages to be exchanged, including a message requesting the desire to communicate securely.

The request and negotiation process described above between the end-point devices in order to establish a secure communications link between the end-point devices is represented diagrammatically in Figure 6:

FIG. 6



The trusted-third-party network device 30, which can be domain name server, recognizes that the unique identifier received from the querying device requires special processing, and it alters its normal operation by, instead of resolving the domain name, for example, establishing "a virtual tunneling association between the originating end and the terminating end of the tunneling association without revealing the identities of both ends of the tunneling association on the public network," Beser at 8:15-20. The trusted-third-party network device 30, i.e., the secure name server, protects the unique identifier from discovery on the Internet by, e.g., encrypting and authenticating communications to/from the device making the query. Beser at 11:20-25.

Thus, Beser shows the step of "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device."

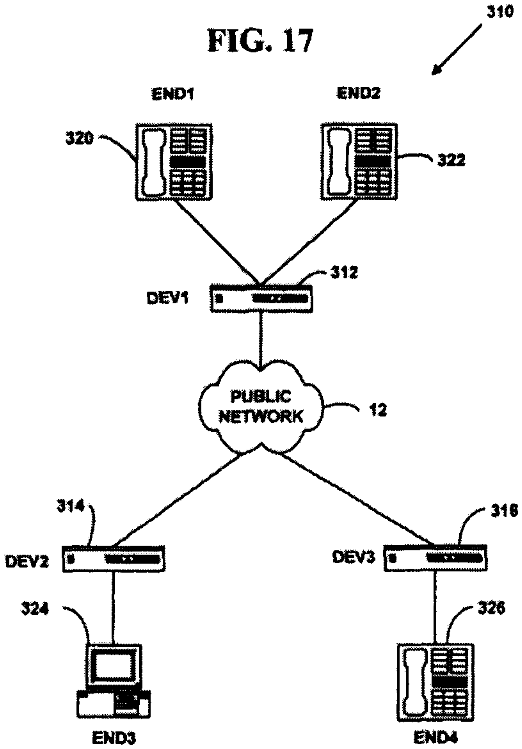
Step (c) of claim 24 further specifies: "sending a message securely from the first device to the second device.

Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Beser also teaches methods that facilitate establishment of a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Following the negotiation described above, Beser discloses that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association." Thus, Beser discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 24 of the '181 patent under 35 U.S.C. § 102(e).

25. Claim 25

Claim 25 depends from claim 24 and specifies "wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link."

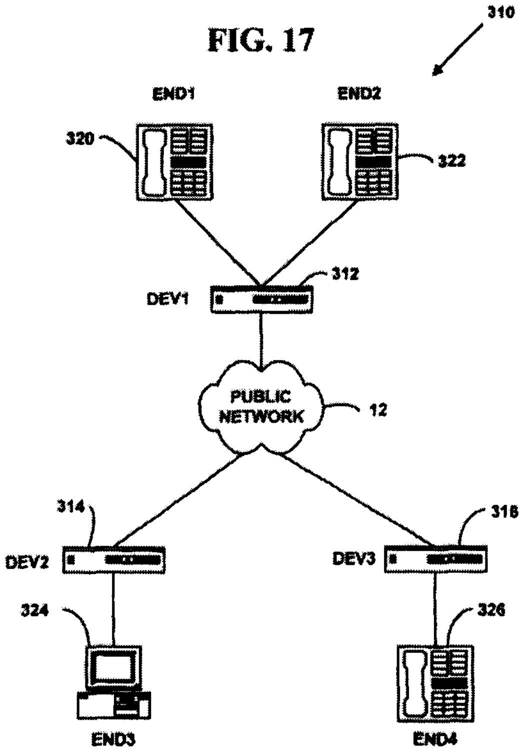
Beser discloses, for example, an embodiment in which the unique identifier, i.e., secure name, is an E.164 telephone number. An E.164 telephone number, Beser explains, "is an ITU recommendation for the assignment of telephone numbers on a world wide basis." Beser at 10:45-48. To that end, Beser shows that "the trusted-third-party network device 30 may be a directory service, owned and operated by a telephone company **that retains a list of E.164 numbers of its subscribers**." Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name.

Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

Beser also teaches methods which facilitate establishment of a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Following the negotiation described above, Beser discloses that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association."

Accordingly, Beser anticipates claim 25 of the '181 patent under 35 U.S.C. § 102(e).

26. Claim 26

Independent claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising:

(a) from the first device requesting and obtaining registration of an unsecured name associated with the first device;

(b) from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;

(c) receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

(d) from the first device sending a message securely from the first device to the second device."

The preamble of claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising." As described in Beser, at 3:1-10:

> [T]he method and system of the present invention may provide for the initiation of a Voice-overInternet-Protocol association between an originating telephony device and a terminating telephony device. The method and system described herein may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication without an increased computational burden.

Thus, Beser discloses "[a] method of using a first device to securely communicate with a second device over a communication network."

Step (a) of claim 26 further specifies: "from the first device requesting and obtaining registration of an unsecured name associated with the first device"

Beser shows that an "unsecure name" is also associated with a "first device." In particular, each network device has associated with it a "public IP address." The "public IP address" is associated with the unique identifier and the first network device 24. As each end-point device have associated therewith a unique identifier, the public IP address—the unsecure name—is thus associated with each end-point device. Or, as explained in Beser :

> A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at Step 116. The second network device 16 is associated with the terminating telephony device 26. This association of the public IP 58 address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30. Beser at 11:25-32.

Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device, together with the public IP address—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name. Beser thus discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device." Beser thus discloses "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Step (b) of claim 26 further specifies: "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device"

Beser discloses, for example, an embodiment in which the unique identifier, i.e., secure name, is an E.164 telephone number. An E.164 telephone number, Beser explains, "is an ITU recommendation for the assignment of telephone numbers on a world wide basis." Beser at 10:45-48. To that end, Beser shows that "the trusted-third-party network device 30 may be a directory service, owned and operated by a telephone company that retains a list of E.164 numbers of its subscribers." Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device, together with the Public IP address—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name. Beser thus discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Step (c) of claim 26 further specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and"

Beser teaches that private IP addresses are assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26) and are negotiated via a negotiation process initiated through the trusted-third-party device 30. Beser at 11:59-62 ("At Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12.") The negotiation and discovery of the private IP addresses are facilitated by the disclosure of the "unique identifier" associated with the terminating devices. Beser at 11:26-37. After negotiation, the private IP addresses are recorded at the trusted-third-party-device:

> Once negotiated, on the first network device 14 is recorded the first private IP 58 address for the originating telephony device 24, and on the second network device 16 is recorded the second private IP 58 address for the terminating telephony device 26. These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective ends of the VoIP association by methods known to those skilled in the art. Beser at 12:28-36.

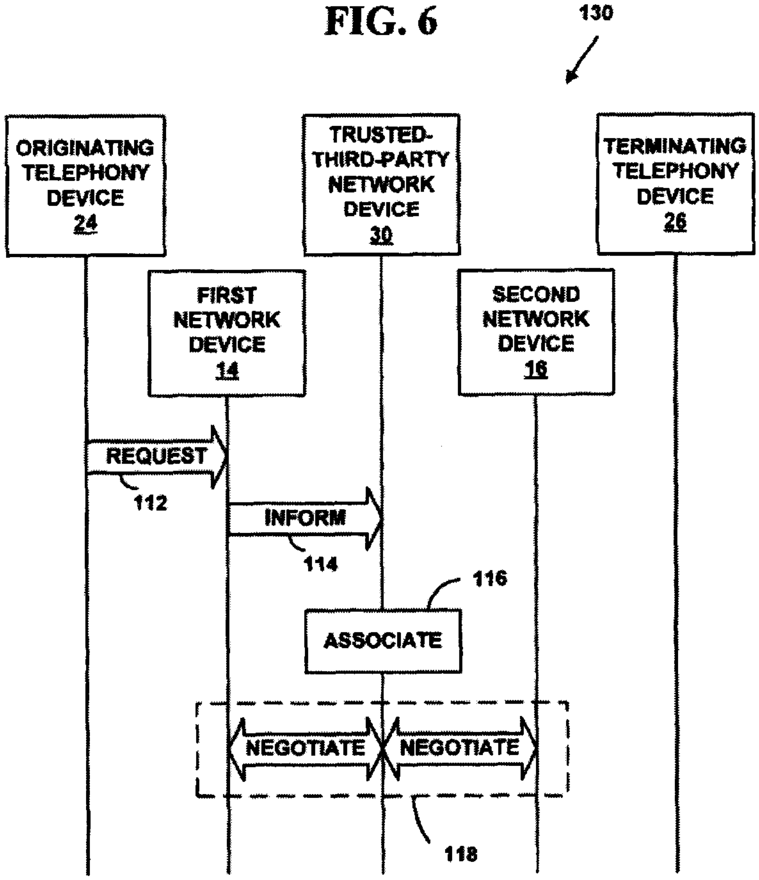
Beser shows that security measures can be utilized which result in receiving, at a network address corresponding to the secure device, a message from a second device of the desire to securely communicate. For example, tunneling—a method of communicating securely—is taught in Beser :

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network.

Beser at 2:6-12. The communications link described in Beser is secure because the "tunneling association hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network," thus preventing public disclosure or interception by hackers. Beser at 2:35-40. Further, under the broadest reasonable interpretation of this claim element, encryption of the communication link is not required. Nevertheless, Beser describes that as another method of securely communicating, "the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec")." Beser at 1:54-56. It was known by one of ordinary skill in the art at the time of the filing of Beser that IPSec security required negotiating Security Associations before secure communications begin, which required messages to be exchanged, including a message requesting the desire to communicate securely.

The request and negotiation process described above between the end-point devices in order to establish a secure communications link between the end-point devices is represented diagrammatically in Figure 6:

FIG. 6



The trusted-third-party network device 30, which can be domain name server, recognizes that the unique identifier received from the querying device requires special processing, and it alters its normal operation by, instead of resolving the domain name, for example, establishing "a virtual tunneling association between the originating end and the terminating end of the tunneling association without revealing the identities of both ends of the tunneling association on the public network," Beser at 8:15-20. The trusted-third-party network device 30, i.e., the secure name server, protects the unique identifier from discovery on the Internet by, e.g., encrypting and authenticating communications to/from the device making the query. Beser at 11:20-25.

Thus, Beser shows the step of "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device."

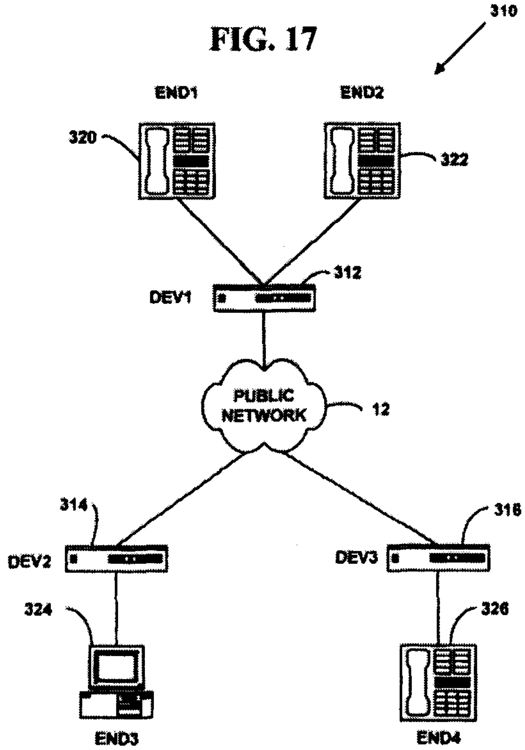
Step (d) of claim 26 further specifies: "from the first device sending a message securely from the first device to the second device."

Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

And, as described in the summary of the invention and detailed throughout, the methods disclosed in Beser facilitate a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Following the negotiation described above, Beser discloses that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association." Thus, Beser discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 26 of the '181 patent under 35 U.S.C. § 102(e).

27. Claim 27

Claim 27 depends from claim 26 and specifies:

(a) "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

(b) wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Step (a) of claim 27 further specifies: "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and"

Beser shows that an "unsecure name" is also associated with a "first device." In particular, each network device has associated with it a "public IP address." The "public IP address" is associated with the unique identifier and the first network device 24. As each end-point device have associated therewith a unique identifier, the public IP address—the unsecure name—is thus associated with each end-point device. Or, as explained in Beser :

> A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at Step 116. The second network device 16 is associated with the terminating telephony device 26. This association of the public IP 58 address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30. Beser at 11:25-32.

Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device, together with the public IP address—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name. Beser thus discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device." Beser thus discloses "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Step (b) of claim 27 further specifies: "wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device"

Beser discloses, for example, an embodiment in which the unique identifier, i.e., secure name, is an E.164 telephone number. An E.164 telephone number, Beser explains, "is an ITU recommendation for the assignment of telephone numbers on a world wide basis." Beser at 10:45-48. To that end, Beser shows that "the trusted-third-party network device 30 may be a directory service, owned and operated by a telephone company that retains a list of E.164 numbers of its subscribers." Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device, together with the Public IP address—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name. Beser thus discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Accordingly, Beser anticipates claim 27 of the '181 patent under 35 U.S.C. § 102(e).

28. Claim 28

Independent claim 28 is directed to "[a] non-transitory machine-readable medium comprising instructions for:

(a) sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

(b) receiving a message containing the network address associated with the secure name of the device; and

(c) sending a message to the network address associated with the secure name of the device using a secure communication link.

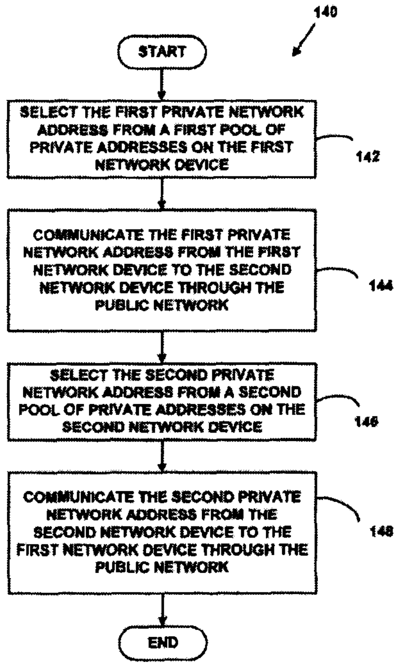
The preamble of claim 28 specifies "[a] non-transitory machine-readable medium comprising instructions. . . ." Beser describes programs, processes, methods systems and apparatus that include, but are not limited to, computer hardware or software. Beser at 25:42-26.

Step (a) of claim 28 further specifies: "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;"

Beser teaches that private IP addresses are assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26) and are negotiated via a negotiation process initiated through the trusted-third-party device 30. Beser at 11:59-62 ("At Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12."). Beser discloses that the trusted-third-party device (3) is a secure name service. Beser at 4:5-11 ("The trusted-third-party 30 may be a back-end service, a domain name server, or the owner/manager of database or directory services.")

In particular, the negotiation process in Beser, as depicted in Figure 7 below, commences by "receiving a request to initiate the VoIP association on a first network device 14 at Step 112. The first network device 14 is associated with the origination telephony device 24, and the request includes a unique identifier for the terminating telephony device 26." Beser at 10:2-6. Further, "[a]t Step 114, a trusted-third-party network device 30 is informed of the request on the public network 12," Beser at 11:9-10, and at Step 116, "a public IP 48 address for a second network device 16 is associated with the unique identifier [supplied by network device 14] for the terminating telephony device 26." Beser at 11:25-29.

FIG. 7


140
START
SELECT THE FIRST PRIVATE NETWORK ADDRESS FROM A FIRST POOL OF PRIVATE ADDRESSES ON THE FIRST NETWORK DEVICE
142
COMMUNICATE THE FIRST PRIVATE NETWORK ADDRESS FROM THE FIRST NETWORK DEVICE TO THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
144
SELECT THE SECOND PRIVATE NETWORK ADDRESS FROM A SECOND POOL OF PRIVATE ADDRESSES ON THE SECOND NETWORK DEVICE
146
COMMUNICATE THE SECOND PRIVATE NETWORK ADDRESS FROM THE SECOND NETWORK DEVICE TO THE FIRST NETWORK DEVICE THROUGH THE PUBLIC NETWORK
148
END

Thus, Beser shows the step of "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

Step (b) of claim 28 further specifies: "receiving a message containing the network address associated with the secure name of the device; and"

Following the negotiation, the first network device (14)—the requesting device—has obtained "the following network addresses: the public network address of the second network device 16, and the private network addresses assigned to the originating 24 and terminating 26 ends of the tunneling association." Beser at 21:38-43. Thus, Beser shows the step of "receiving a message containing the network address associated with the secure name of the device."

Step (c) of claim 28 further specifies: "sending a message to the network address associated with the secure name of the device using a secure communication link."

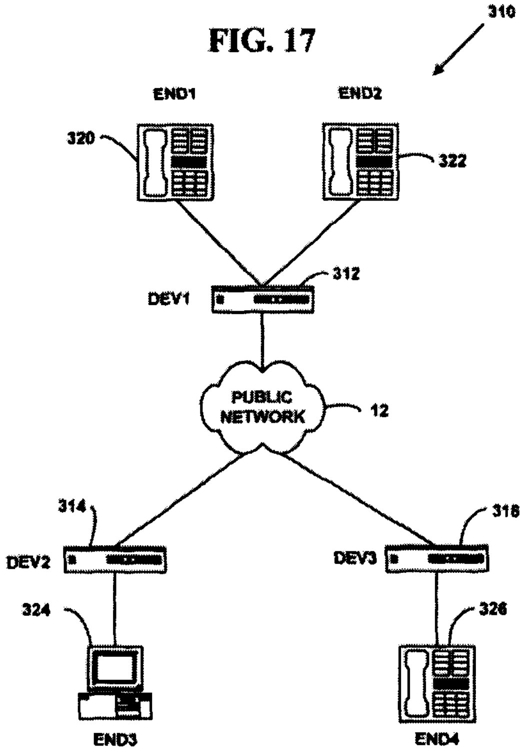
Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio

> applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

And, as described in the summary of the invention and detailed throughout, the methods disclosed in Beser facilitate a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Following the negotiation described above, Beser discloses that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association." Thus, Beser discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 28 of the '181 patent under 35 U.S.C. § 102(e).

29. Claim 29

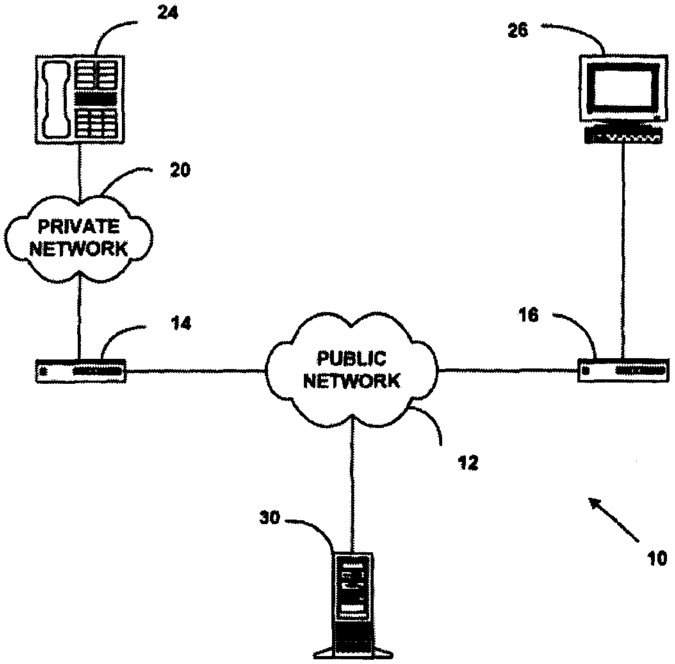
Independent claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

(a) receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and

(b) sending a message securely from the first device to the second device.

The preamble of claim 29 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name . . . ." Beser describes programs, processes, methods systems and apparatus that include, but are not limited to, computer hardware or software. Beser at 25:42-26. In particular, Beser teaches—as shown below in Figure 1—a first network device (14), a second network device (16), two end-point devices (24, 26), which may be Voice Over Internet Protocol ("VoIP") phones, and a trusted third party device (30):

FIG. 1



The first network device (14) and second network device (16) may be modified routers or gateways, and the trusted-third-party device 30 may be "a back-end service, a domain name server or the owner/manager of database or directory services." Beser at 4:5-11. Beser further explains that end-point devices (24, 26) are "originating and terminating ends of data flow."

Beser at 4:43-44. Beser indicates that these end-point devices can include telephony and multimedia devices. For example, Beser explains that:

> Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:47-50.

First and second network devices (14, 16) and end-point devices (24, 26) have associated therewith both secure and unsecure names. For example, end-point devices (24, 26) each have an secure name that comprises a "unique identifier" that is registered with the trusted-third-party device (30). Beser at 11:28-32 ("The second network device 16 is associated with the terminating telephony device 26. This association of the public IP address for the second network device 16 with the unique identifier is made on the trusted-third-party network device 30."). The unique identifier may be "any of a dial-up number, an electronic mail address, or a domain name." Beser at 10:37-41. Thus, Beser discloses "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name

Step (a) of claim 29 further specifies: "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and"

Beser teaches that private IP addresses are assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26) and are negotiated via a negotiation process initiated through the trusted-third-party device 30. Beser at 11:59-62 ("At Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12.") The negotiation and discovery of the private IP addresses are facilitated by the disclosure of the "unique identifier" associated with the terminating devices. Beser at 11:26-37. After negotiation, the private IP addresses are recorded at the trusted-third-party-device:

> Once negotiated, on the first network device 14 is recorded the first private IP 58 address for the originating telephony device 24, and on the second network device 16 is recorded the second private IP 58 address for the terminating telephony device 26. These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective ends of the VoIP association by methods known to those skilled in the art.

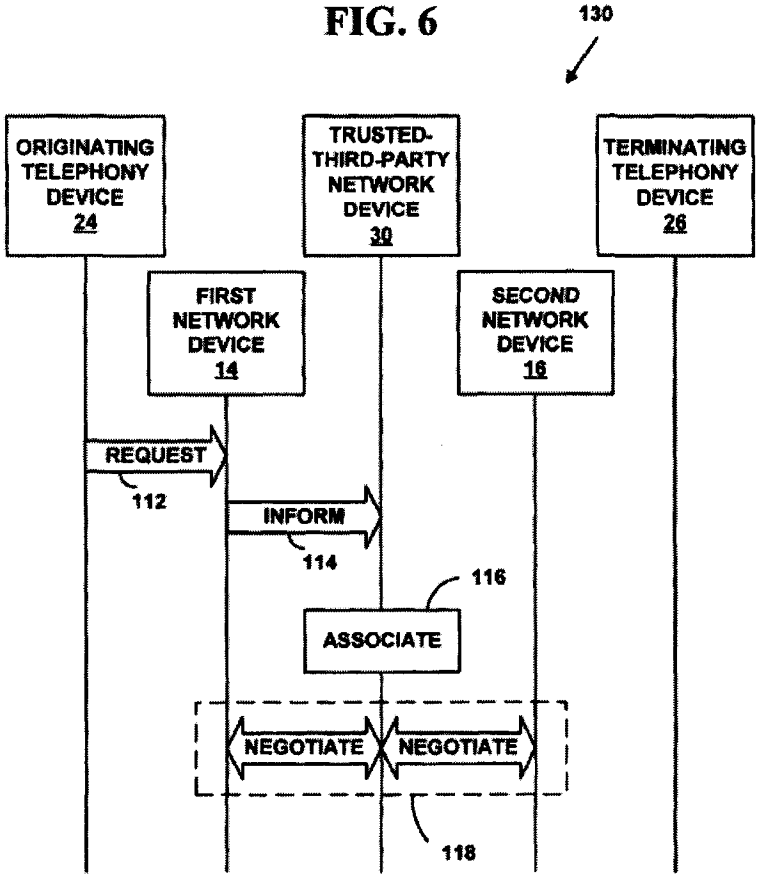
Beser at 12:28-36. Beser shows that security measures can be utilized which result in receiving, at a network address corresponding to the secure device, a message from a second device of the desire to securely communicate. For example, tunneling—a method of communicating securely—is taught in Beser :

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network.

Beser at 2:6-12. The communications link described in Beser is secure because the "tunneling association hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network," thus preventing public disclosure or interception by hackers. Beser at 2:35-40. Further, under the broadest reasonable interpretation of this claim element, encryption of the communication link is not required. Nevertheless, Beser describes that as another method of securely communicating, "the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec")." Beser at 1:54-56. It was known by one of ordinary skill in the art at the time of the filing of Beser that IPSec security required negotiating Security Associations before secure communications begin, which required messages to be exchanged, including a message requesting the desire to communicate securely.

The request and negotiation process described above between the end-point devices in order to establish a secure communications link between the end-point devices is represented

FIG. 6



diagrammatically in Figure 6:

> The trusted-third-party network device 30, which can be domain name server, recognizes that the unique identifier received from the querying device requires special processing, and it alters its normal operation by, instead of resolving the domain name, for example, establishing "a virtual tunneling association between the originating end and the terminating end of the tunneling association without revealing the identities of both ends of the tunneling association on the public network," Beser at 8:15-20. The trusted-third-party network device 30, i.e., the secure name server, protects the unique identifier from discovery on the Internet by, e.g., encrypting and authenticating communications to/from the device making the query. Beser at 11:20-25.

Further, Beser discloses, for example, an embodiment in which the unique identifier, i.e., secure name, is an E.164 telephone number. An E.164 telephone number, Beser explains, "is an ITU recommendation for the assignment of telephone numbers on a world wide basis." Beser at 10:45-48. To that end, Beser shows that "the trusted-third-party network device 30 may be a directory service, owned and operated by a telephone company that retains a list of E.164 numbers of its subscribers." Further, Beser shows that the "association of the public IP 58 address for the second network device 16 with the unique identifier" provided by end-point requesting device "is made by the trusted-third-party network 30." This association—i.e., the association of the secure name with the terminating device, together with the Public IP address—is only possible because each device (include the originating device) has already requested and obtained registration of its secure name. Beser thus discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Thus, Beser shows the step of "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered."

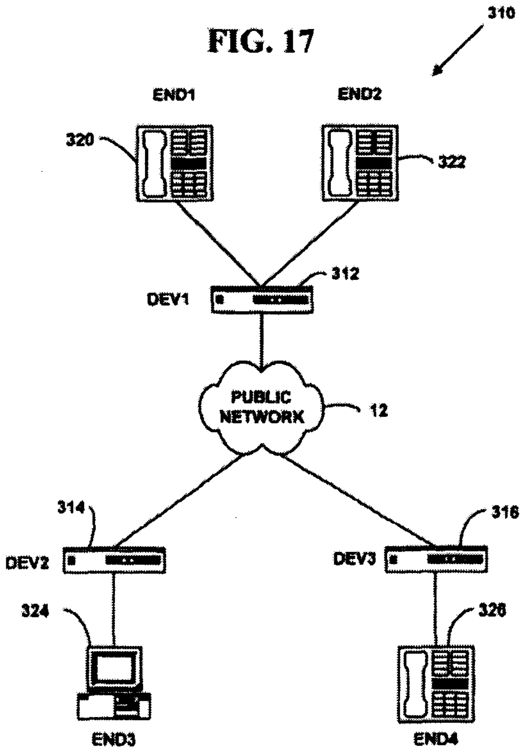
Step (b) of claim 29 further specifies: "sending a message securely from the first device to the second device."

Beser shows that after security methods are implemented, VoIP, or any of the other multimedia communications disclosed, may commence. For example, Beser explains:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

And, as described in the summary of the invention and detailed throughout, the methods disclosed in Beser facilitate a secure communication link between two networked devices. For example, Beser graphically depicts an exemplary configuration of network devices in Figure 17:

FIG. 17



Following the negotiation described above, Beser discloses that "[a]n outgoing message from END1 320 is associated with private IP address for END1 320 at the transmitting end of the tunneling association [i.e., secure communication link] between END1 320 and END3 324. The network address table associates this private IP 58 address with the private IP 58 address for END3 324 at the receiving end of this tunneling association." Thus, Beser discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 29 of the '181 patent under 35 U.S.C. § 102(e).

B. Ground No. 2: Claim 18 is Unpatentable under 35 USC § 103 as Being Obvious Based on Beser in View of RFC 2401

1. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

A person of ordinary skill in the art would immediately recognize from Beser that all communications within an IP tunnel between a first and second network device (i.e., both to initiate the tunnel and following establishment of the IP tunnel) could be authenticated and could also be encrypted other than for certain high traffic applications. *See* Beser at 1:56–2:15. Beser also shows that the IPsec protocol can and should be used to handle the encryption of the traffic being sent through the IP tunnel. Beser at 1:54-56.

RFC 2401 explains, at 30-31, that IPsec evaluates IP packets to determine whether encryption and authentication is required. Specifically, IP packets are to be evaluated as follows:

> In a security gateway or BITW implementation (and in many BITS implementations), each outbound packet is compared against the SPD to determine what processing is required for the packet. If the packet is to be discarded, this is an auditable event. If the traffic is allowed to bypass IPsec processing, the packet continues through "normal" processing for the environment in which the IPsec processing is taking place. If IPsec processing is required, the packet is either mapped to an existing SA (or SA bundle), or a new SA (or SA bundle) is created for the packet. Since a packet's selectors might match multiple policies or multiple extant SAs and since the SPD is ordered, but the SAD is not, IPsec MUST:
>
> 1. Match the packet's selector fields against the outbound policies in the SPD to locate the first appropriate policy, which will point to zero or more SA bundles in the SAD.
>
> 2. Match the packet's selector fields against those in the SA bundles found in (1) to locate the first SA bundle that matches. If no SAs were found or none match, create an appropriate SA bundle and link the SPD entry to the SAD entry. If no key management entity is found, drop the packet.
>
> 3. Use the SA bundle found/created in (2) to do the required IPsec processing, e.g., authenticate and encrypt.
>
> In a host IPsec implementation based on sockets, the SPD will be consulted whenever a new socket is created, to determine what, if any, IPsec processing will be applied to the traffic that will flow on that socket.

Thus, the scheme by which IPsec functions will evaluate the IP packet as it is leaving the starting node, and if a policy dictates that the packet requires IPsec handling, then authentication and encryption will be applied automatically to create the IPsec relationship with the destination. If the applicable policy does not require IPsec handling, then the packet is passed through for normal handling by the involved network devices. This handling is automatic, and does not require user intervention, other than as needed to satisfy authentication requirements.

Beser, in view of RFC 2401, thus would have rendered obvious to a person of ordinary skill in the art the adaption of the Beser IP tunneling process to incorporate authentication and encryption of all IP traffic between the first and second network devices, yielding a method for establishing a secure communication linked between a first network device and a second network device.

Accordingly, Beser, in view of RFC 2401, renders obvious claim 18 of the '181 patent under 35 U.S.C. § 103.

V. DETAILED EXPLANATION OF MANNER OF APPLYING MATTAWAY TO CLAIMS 1-29 AND PROPOSED REJECTIONS BASED ON GROUND NOS. 3-5

Exhibit C2 correlates each of claims 1-29 of the '181 patent with the section of the present request that sets out the detailed basis for anticipation and/or obviousness of the claim, along with an identification of the relevant portions of Mattaway, alone or in conjunction with Beser and RFC 2401. Requester notes that any emphasis indicated in quotations or other citations (e.g., as shown in bold faced text) has been added and is not original to the references cited in this section, unless otherwise noted.

C. Ground No. 3: Claims 1-2, 5-9, 12-17, and 19-22, 24-29 are anticipated under 35 U.S.C. § 102(e) based on Mattaway

Mattaway describes methods and systems for establishing a secure communication link between two devices across a public network such as the Internet. Mattaway discloses a computer program for use in a networked system for establishing a secure point-to-point communication link between two devices. For example, the disclosed methods and systems permit users to utilize the breadth and security of the Internet in order to facilitate audio and video communications. The WebPhone application, seen below, is an exemplary embodiment.

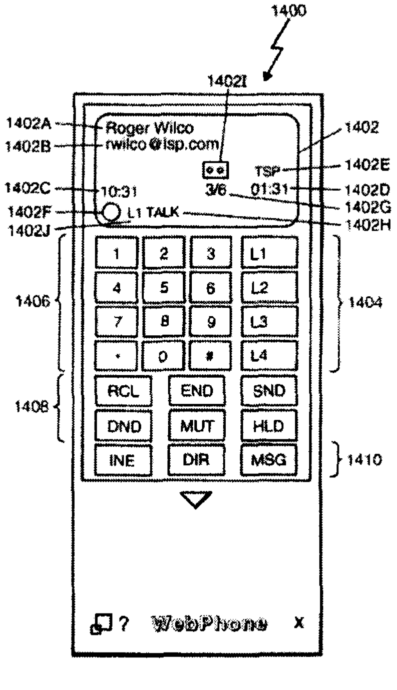


Figure 14

1. Claim 1

Claim 1 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising":

(a) receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and

(b) sending a message over a secure communication link from the first device to the second device.

The preamble of claim 1 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name . . . ." Mattaway teaches, for example:

> a computer program product for use with a computer system compris[ing] a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process form the server, and program code responsive to the network protocol address of the second client process for establishing a point-to-point communications link between the first client process and the second client process. Mattaway at 3:8-20.

Mattaway teaches a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20, as shown in Figure 1:

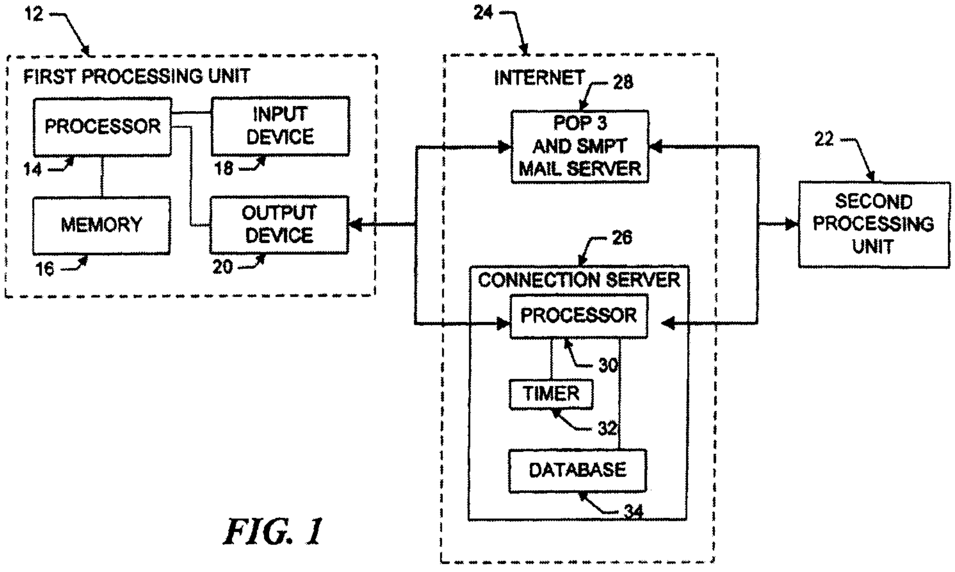


FIG. 1

Mattaway discloses that the first and second processing units (12, 22) may comprise VOIP ("Voice Over Internet Protocol") software that enable communications with other, for example, processing unites:

> In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, 40 Boca Raton, Fla., which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

The connection server 26 acts as a secure name service by storing the network address (e.g., the IP address of the callee) associated with the secure name of the callee's device, i.e., the callee's E-mail address. The secure name is made secure, for example, because it is protected behind a "firewall server 1522," which "is a single firewall mechanism which protects unauthorized access from network 1530 into global server 1500." Mattaway at 17:44-48. Mattaway also provides a disclosure in TABLE 9 that describes the "eemailAddr" element as an encrypted email Address. Mattaway at 40:27.

Mattaway shows that the disclosed system and methods can include an unsecured name, such as a user's "alias." Mattaway at 11:13-15. The party's name may be stored in a "personal information directory" of other parties, Mattaway at 26:43-55, and "a party name field 1402A" will "display[] the name of the caller when an incoming call arrives," Mattaway at 26:45-47, and will when an outgoing call is made, so long as the party name has been stored in the directory. Mattaway at 26:63-67.

Thus, Mattaway discloses "a non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name."

Step (a) of Claim 1 specifies: "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and"

Mattaway describes two protocols for establishing point-to-point secure communications between two networked devices. The first protocol utilizes a connection server to implement a one-to-one mapping of E-mail addresses to Internet Protocol addresses." Mattaway at 18:41-45. The basic steps of this process are described in Figure 16A, which identifies the sending and receipt of a message of the intent to securely communicate. The receipt is represented by the <CONNECT ACK> packet, illustrated by decisional block 1616 and process block 1618:

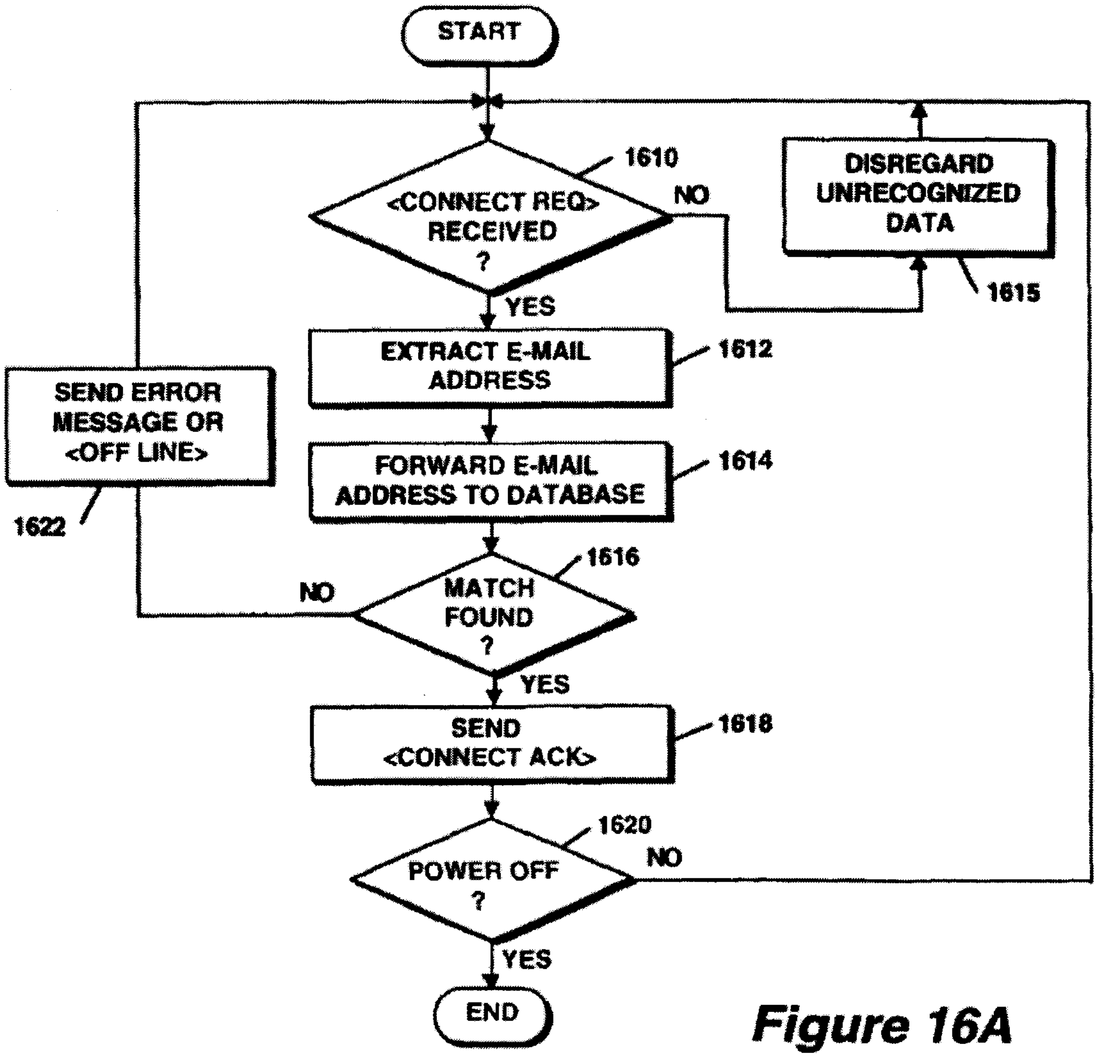


Figure 16A

Mattaway also describes a second protocol that involves sending messages via a mail server in order to implement the disclosed point-to-point communications protocol. For example:

> As described above, the first processing unit 12 may send the <ConnectReq> message in response to an unsuccessful attempt to perform the primary point-to-point Internet protocol. Alternatively, the first processing unit 12 may send the <ConnectReq> message in response to the first user initiating a SEND command or the like After the <ConnectRequest> message via E-mail is sent, the first processing unit 12 opens a socket and waits to detect a response from the second processing unit 22. A timeout timer, such as timer 32, may be set by the first processing unit 12, in a manner known in the art, to wait for a predetermined duration to receive a <ConnectOK> signal. The processor 14 of the first processing unit 12 may cause 40 the output device 20 to output a Ring signal to the user, such as an audible ringing sound, about every 3 seconds. Mattaway at 8:25-44.

Thus, Mattaway discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Step (b) of claim 1 specifies: "sending a message over a secure communication link from the first device to the second device."

> Upon retrieval of the IP address of the callee, "the first processing unit 12 may then directly establish the point-to-point Internet communications with the callee using the IP address of the callee." Mattaway at 7:33-37. Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Thus, Mattaway discloses "sending a message over a secure communication link from the first device to the second device." Accordingly, Mattaway anticipates claim 1 of the '181 patent under 35 U.S.C. § 102(e).

2. Claim 2

Independent claim 2 is directed to [a] method of using a first device to communicate with a second device having a secure name, the method comprising:

> (a) from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;
>
> (b) at the first device, receiving a message containing the network address associated with the secure name of the second device; and
>
> (c) from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

The preamble of claim 2 specifies "[a] method of using a first device to communicate with a second device having a secure name . . . ." Mattaway teaches, for example:

> a computer program product for use with a computer system compris[ing] a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process form the server, and program code responsive to the network protocol address of the second client process for establishing a point-to-point communications link between the first client process and the second client process. Mattaway at 3:8-20.

Mattaway teaches a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20, as shown in Figure 1:

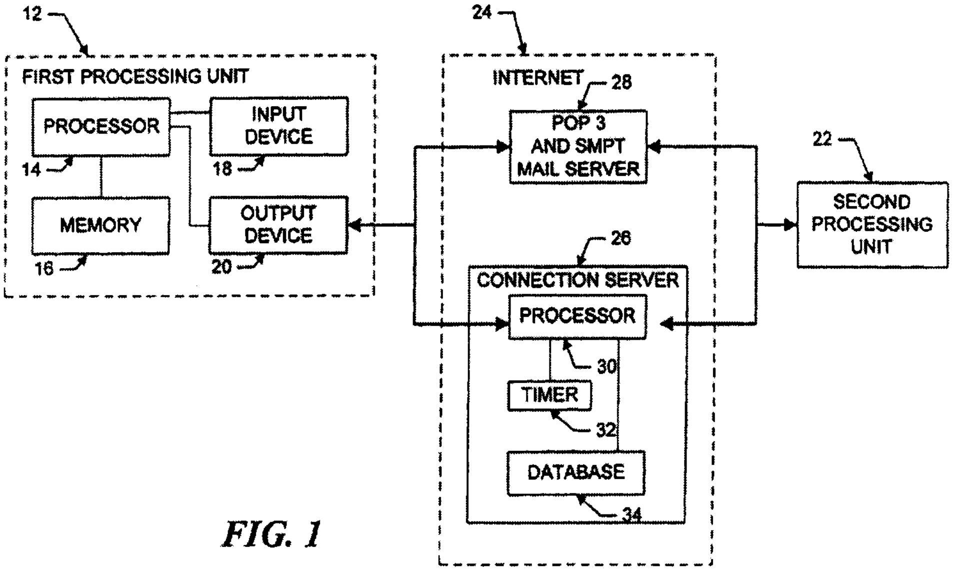


FIG. 1

Mattaway discloses that the first and second processing units (12, 22) may comprise VOIP ("Voice Over Internet Protocol") software that enable communications with other, for example, processing unites:

> In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, 40 Boca Raton, Fla., which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

Thus, Mattaway discloses "[a] method of using a first device to communicate with a second device having a secure name."

Step (a) of claim 2 further specifies: "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Mattaway shows that a first user must query the connection in order to obtain the network address associated with the secure name of the second device. For example:

> The first processing unit 12 then sends a query, including the E-mail address of the callee, to the connection server 26. The connection server 26 then searches the database 34 to determine whether the callee is logged-in by finding any stored information corresponding to the callee's E-mail address indicating that the callee is active and on-line. If the callee is active and on-line, the connection server 26 then performs the primary point-to-point

> Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. Mattaway at 7:24-37.

The connection server 26 acts as a secure name service by storing the network address (e.g., the IP address of the callee) associated with the secure name of the callee's device, i.e., the callee's E-mail address. The secure name is made secure, for example, because it is protected behind a "firewall server 1522," which "is a single firewall mechanism which protects unauthorized access from network 1530 into global server 1500." Mattaway at 17:44-48. Mattaway also provides a disclosure in TABLE 9 that describes the "eemailAddr" element as an encrypted email Address. Mattaway at 40:27. Thus, Mattaway shows the step of "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Step (b) of claim 2 further specifies: "at the first device, receiving a message containing the network address associated with the secure name of the second device"

Mattaway shows that the first device will receive a message containing the network address associated with the secure name of the second device. For example:

> If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. Mattaway at 7:32-37.

Thus, Mattaway shows the step of "at the first device, receiving a message containing the network address associated with the secure name of the second device."

Step (c) of claim 2 further specifies: "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

Upon retrieval of the IP address of the callee, "the first processing unit 12 may then directly establish the point-to-point Internet communications with the callee using the IP address of the callee." Mattaway at 7:33-37. Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Accordingly, Mattaway anticipates claim 2 of the '181 patent under 35 U.S.C. § 102(e).

3. Claim 5

Claim 5 of the '181 patent depends from claim 2, and specifies "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form."

Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Accordingly, Mattaway anticipates claim 5 of the '181 patent under 35 U.S.C. § 102(e).

4. Claim 6

Claim 6 depends from claim 2, and specifies that the step of "further including decrypting the message."

Because Mattaway discloses that that "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks," Mattaway at 25:32-34, it inherently discloses the ability to decrypt those encrypted audio communications.

Accordingly, Mattaway anticipates claim 6 of the '181 patent under 35 U.S.C. § 102(e).

5. Claim 7

Claim 7 of the '181 patent depends from claim 2, and specifies "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed."

Mattaway discloses a plurality of protocols used to implement the sending and receiving of messages, for example, "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) 45 on top of the IP." Mattaway at 6:37-45. *See also* Mattaway at 17:1-5 ("The sockets 1322 are accessible by network 1330 through a number of protocols including Internet Protocol (IP) 1332, Transmission Control Protocol (TCP) 1334, RealTime Protocol (RTP) 1336 and User Datagram Protocol (UDP) 1338."). Such protocols may be implemented in order to engage in point-to-point communications regardless of the security measures utilized.

Accordingly, Mattaway anticipates claim 7 of the '181 patent under 35 U.S.C. § 102(e).

6. Claim 8

Claim 8 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

Mattaway shows that the first device will receive a message containing the network address associated with the secure name of the second device. For example:

> "If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12." Mattaway at 7:32-37.

Accordingly, Mattaway anticipates claim 8 of the '181 patent under 35 U.S.C. § 102(e).

7. Claim 9

Claim 9 depends from claim 2 and specifies that "further including automatically initiating the secure communication link after it is enabled."

Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34. Further, nothing in the specification suggests user interaction is involved regarding the underlying actions of the computer programs that set up the encrypted audio communications.

Accordingly, Mattaway anticipates claim 9 of the '181 patent under 35 U.S.C. § 102(e).

8. Claim 12

Claim 12 depends from claim 2 and specifies "wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols."

Mattaway discloses a plurality of protocols used to implement the sending and receiving of messages, for example, "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) 45 on top of the IP." Mattaway at 6:37-45. *See also* Mattaway at 17:1-5 ("The sockets 1322 are accessible by network 1330 through a number of protocols including Internet Protocol (IP) 1332, Transmission Control Protocol (TCP) 1334, RealTime Protocol (RTP) 1336 and User Datagram Protocol (UDP) 1338.").

Accordingly, Mattaway anticipates claim 12 of the '181 patent under 35 U.S.C. § 102(e).

9. Claim 13

Claim 13 depends from claim 2 and specifies "wherein the receiving and sending of messages through the secure communication link includes multiple sessions."

Mattaway discloses that each call, i.e., session, "may be assigned a successive session number in sequence, which may be used by the respective processing unit to associate the call with one of the SLIP/PPP lines, to associate a <ConnectOK> response signal from a <Connect Request> signal, and to allow for multiplexing and demultiplexing of inbound and outbound conversations on conference lines . . . ."

Accordingly, Mattaway anticipates claim 13 of the '181 patent under 35 U.S.C. § 102(e).

10. Claim 14

Claim 14 depends from claim 2 and specifies "further including supporting a plurality of services over the secure communication link."

Mattaway discloses a plurality of protocols used to implement the sending and receiving of messages, for example, "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) 45 on top of the IP." Mattaway at 6:37-45. *See also* Mattaway at 17:1-5 ("The sockets 1322 are accessible by network 1330 through a number of protocols including Internet Protocol (IP) 1332, Transmission Control Protocol (TCP) 1334, RealTime Protocol (RTP) 1336 and User Datagram Protocol (UDP) 1338.")

Mattaway also discloses a plurality of application programs, including the "WEBPHONE® Internet telephony application," Mattaway at 4:38-41, which is supported by such graphical user interface programs as "Windows 3.1" or "OS/2 and OS/2 Warp." Mattaway at 5:50-54.

Accordingly, Mattaway anticipates claim 14 of the '181 patent under 35 U.S.C. § 102(e).

11. Claim 15

Claim 15 depends from claim 14 and specifies "wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof."

Mattaway discloses a plurality of protocols used to implement the sending and receiving of messages, for example, "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) 45 on top of the IP." Mattaway at 6:37-45. *See also* Mattaway at 17:1-5 ("The sockets 1322 are accessible by network 1330 through a number of protocols including Internet Protocol (IP) 1332, Transmission Control Protocol (TCP) 1334, RealTime Protocol (RTP) 1336 and User Datagram Protocol (UDP) 1338.")

Mattaway also discloses a plurality of application programs, including the "WEBPHONE® Internet telephony application," Mattaway at 4:38-41, which is supported by such graphical user interface programs as "Windows 3.1" or "OS/2 and OS/2 Warp." Mattaway at 5:50-54.

Accordingly, Mattaway anticipates claim 15 of the '181 patent under 35 U.S.C. § 102(e).

12. Claim 16

Claim 16 depends from claim 15 and specifies "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof."

The first processing unit "may execute the WEBPHONE® Internet telephony application . . . which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein." Mattaway at 4:38-41. In addition, the "WebPhone API 1326 transfers real-time and streamed audio via the UDP protocol and real-time audio and video data via the UDP and RTP protocols." Mattaway at 17:5-9.

Accordingly, Mattaway anticipates claim 16 of the '181 patent under 35 U.S.C. § 102(e).

13. Claim 17

Claim 17 depends from claim 15 and specifies "wherein the plurality of services comprises audio, video or a combination thereof."

Mattaway shows that the "[t]he first processing unit "may execute the WEBPHONE® Internet telephony application . . . which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein." Mattaway at 4:38-41. Further, the "WebPhone API 1326 transfers real-time and streamed **audio** via the UDP protocol and real-time **audio and video** data via the UDP and RTP protocols." Mattaway at 17:5-9.

Accordingly, Mattaway anticipates claim 17 of the '181 patent under 35 U.S.C. § 102(e).

14. Claim 19

Claim 19 depends from claim 2 and specifies "wherein the first device is a computer, and the steps are performed on the computer."

Mattaway shows that "[t]he first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20." Mattaway at 4:22-24. The first processing unit "may execute the WEBPHONE® Internet telephony application . . . which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein." Mattaway at 4:37-42.

Accordingly, Mattaway anticipates claim 19 of the '181 patent under 35 U.S.C. § 102(e).

15. Claim 20

Claim 20 depends from claim 2 and specifies "wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network."

Mattaway shows that "[t]he first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20. The output device 20 includes at 25 least one modem capable of, for example, 14.4 Kilobit-per second communications and operatively connected via wired and/or wireless communication connections to the Internet or other computer networks such as an Intranet, i.e., a private computer network." Mattaway at 4:22-29. The first processing unit "may execute the WEBPHONE® Internet telephony application . . . which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein." Mattaway at 4:37-42.

Accordingly, Mattaway anticipates claim 20 of the '181 patent under 35 U.S.C. § 102(e).

16. Claim 21

Claim 21 depends from claim 2 and specifies "further including providing an unsecured name associated with the device."

Mattaway shows that the disclosed system and methods can include an unsecured name, such as a user's "alias." Mattaway at 11:13-15. The party's name may be stored in a "personal information directory" of other parties, Mattaway at 26:43-55, and "a party name field 1402A" will "display[] the name of the caller when an incoming call arrives," Mattaway at 26:45-47, and will when an outgoing call is made, so long as the party name has been stored in the directory. Mattaway at 26:63-67.

Accordingly, Mattaway anticipates claim 21 of the '181 patent under 35 U.S.C. § 102(e).

17. Claim 22

Claim 22 depends from claim 2 and specifies "wherein the secure name is registered prior to the step of sending a message to a secure name service."

Accordingly, Mattaway anticipates claim 22 of the '181 patent under 35 U.S.C. § 102(e).

18. Claim 24

Independent claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network, the method comprising:

(a) at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;

(b) receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and

(c) sending a message securely from the first device to the second device."

The preamble is directed to "[a] method of using a first device to securely communicate with a second device over a communication network. Mattaway teaches, for example:

> a computer program product for use with a computer system compris[ing] a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process form the server, and program code responsive to the network protocol address of the second client process for establishing a point-to-point communications link between the first client process and the second client process. Mattaway at 3:8-20.

Mattaway teaches a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20, as shown in Figure 1:

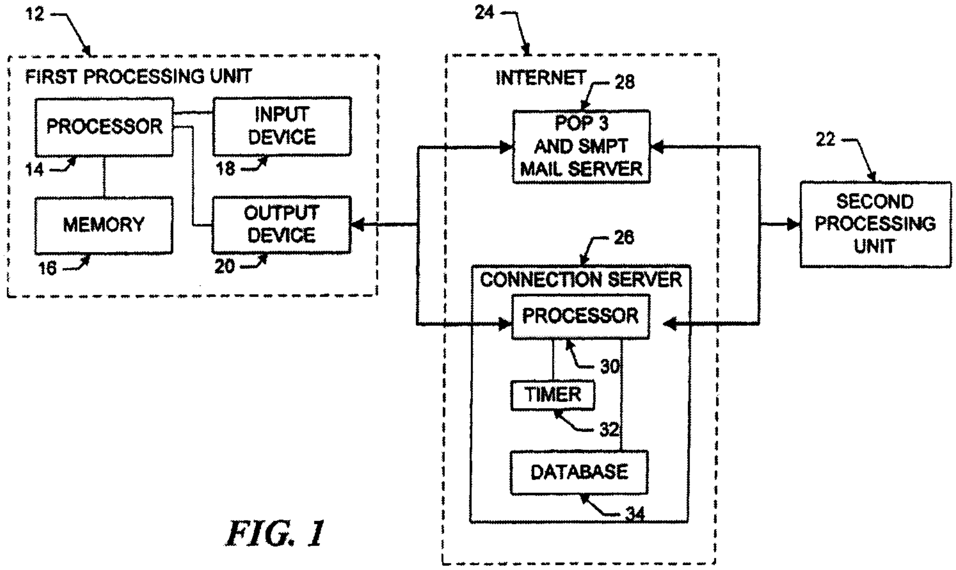


FIG. 1

Mattaway discloses that the first and second processing units (12, 22) may comprise VOIP ("Voice Over Internet Protocol") software that enable communications with other, for example, processing unites:

> In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, 40 Boca Raton, Fla., which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

Thus, Mattaway discloses "[a] method of using a first device to securely communicate with a second device over a communication network."

Step (a) of claim 24 further specifies: "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address"

Mattaway discloses a registration process in which the first processing unit registers a secure name associated with an IP address. For example:

> Upon the first user initiating the point-to-point Internet protocol when the first user is logged on to the Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server 26. The connection server 26 then stores these addresses in the database 34 . . . . Mattaway at 6:60-65.

Thus, Mattaway shows the step of "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

Step (b) of claim 24 further specifies: "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device."

Mattaway shows that the first device will receive a message from a second device of the desire to securely communicate. For example:

> "If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12."
> Mattaway at 7:32-37.

Mattaway describes two protocols for establishing point-to-point secure communications between two networked devices. The first protocol utilizes a connection server to implement a one-to-one mapping of E-mail addresses to Internet Protocol addresses." Mattaway at 18:41-45. The basic steps of this process are described in Figure 16A, which identifies the sending and receipt of a message of the intent to securely communicate. The receipt is represented by the <CONNECT ACK> packet, illustrated by decisional block 1616 and process block 1618:

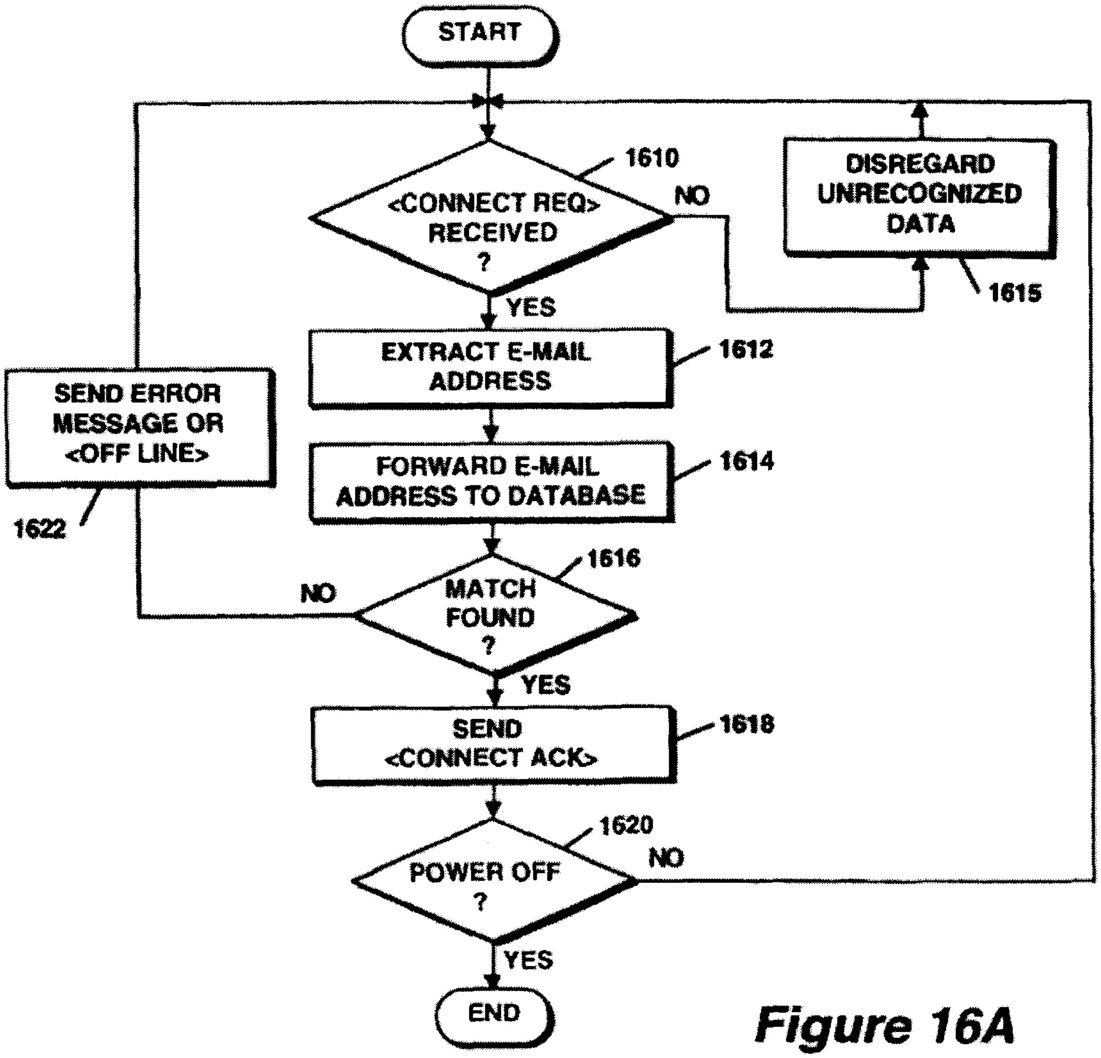


Figure 16A

Mattaway also describes a second protocol that involves sending messages via a mail server in order to implement the disclosed point-to-point communications protocol. For example:

> As described above, the first processing unit 12 may send the <ConnectReq> message in response to an unsuccessful attempt to perform the primary point-to-point Internet protocol. Alternatively, the first processing unit 12 may send the <ConnectReq> message in response to the first user initiating a SEND command or the like. After the <ConnectRequest> message via E-mail is sent, the first processing unit 12 opens a socket and waits to detect a response from the second processing unit 22. A timeout timer, such as timer 32, may be set by the first processing unit 12, in a manner known in the art, to wait for a predetermined duration to receive a <ConnectOK> signal. The processor 14 of the first processing unit 12 may cause 40 the output device 20 to output a Ring

> signal to the user, such as an audible ringing sound, about every 3 seconds. Mattaway at 8:25-44.

Thus, Mattaway discloses "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device."

Step (c) of claim 24 further specifies: "sending a message securely from the first device to the second device."

Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Accordingly, Mattaway anticipates claim 24 of the '181 patent under 35 U.S.C. § 102(e).

19. Claim 25

Claim 25 depends from claim 24 and specifies "wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link."

Mattaway discloses a registration process in which the first processing unit registers a secure name associated with an IP address. For example:

> Upon the first user initiating the point-to-point Internet protocol when the first user is logged on to the Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server 26. The connection server 26 then stores these addresses in the database 34 . . . . Mattaway at 6:60-65.

Mattaway also shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34. Thus, Mattaway discloses the step of "sending a message securely from the first device to the second device."

Accordingly, Mattaway anticipates claim 25 of the '181 patent under 35 U.S.C. § 102(e).

20. Claim 26

Independent claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising:

> (a) from the first device requesting and obtaining registration of an unsecured name associated with the first device;

(b) from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;

(c) receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

(d) from the first device sending a message securely from the first device to the second device."

The preamble describes "[a] method of using a first device to communicate with a second device over a communication network, the method . . . ." Mattaway teaches, for example:

> a computer program product for use with a computer system compris[ing] a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process form the server, and program code responsive to the network protocol address of the second client process for establishing a point-to-point communications link between the first client process and the second client process. Mattaway at 3:8-20.

Mattaway teaches a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20, as shown in Figure 1:

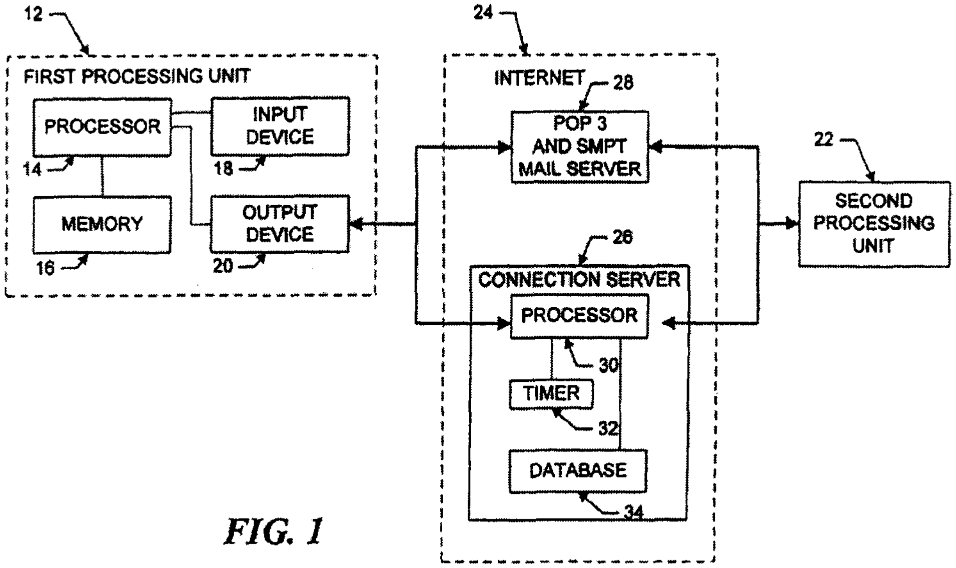


FIG. 1

Mattaway discloses that the first and second processing units (12, 22) may comprise VOIP ("Voice Over Internet Protocol") software that enable communications with other, for example, processing unites:

> In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, 40 Boca Raton, Fla., which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

Thus, Mattaway discloses "[a] method of using a first device to communicate with a second device over a communication network."

Step (a) of claim 26 further specifies: "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Mattaway shows that the disclosed system and methods can include an unsecured name, such as a user's "alias." Mattaway at 11:13-15. The party's name may be stored in a "personal information directory" of other parties, Mattaway at 26:43-55, and "a party name field 1402A" will "display[] the name of the caller when an incoming call arrives," Mattaway at 26:45-47, and will when an outgoing call is made, so long as the party name has been stored in the directory. Mattaway at 26:63-67.

Thus, Mattaway discloses the step of "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Step (b) of claim 26 further specifies: "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Mattaway discloses a registration process in which the first processing unit registers a secure name associated with an IP address. For example:

> Upon the first user initiating the point-to-point Internet protocol when the first user is logged on to the Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server 26. The connection server 26 then stores these addresses in the database 34 . . . . Mattaway at 6:60-65.

Thus, Mattaway discloses the step of "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device."

Step (c) of claim 26 further specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device."

Mattaway shows that the first device will receive a message from a second device of the desire to securely communicate. For example:

> If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. Mattaway at 7:32-37.

Mattaway describes two protocols for establishing point-to-point secure communications between two networked devices. The first protocol utilizes a connection server to implement a one-to-one mapping of E-mail addresses to Internet Protocol addresses." Mattaway at 18:41-45. The basic steps of this process are described in Figure 16A, which identifies the sending and receipt of a message of the intent to securely communicate. The receipt is represented by the <CONNECT ACK> packet, illustrated by decisional block 1616 and process block 1618:

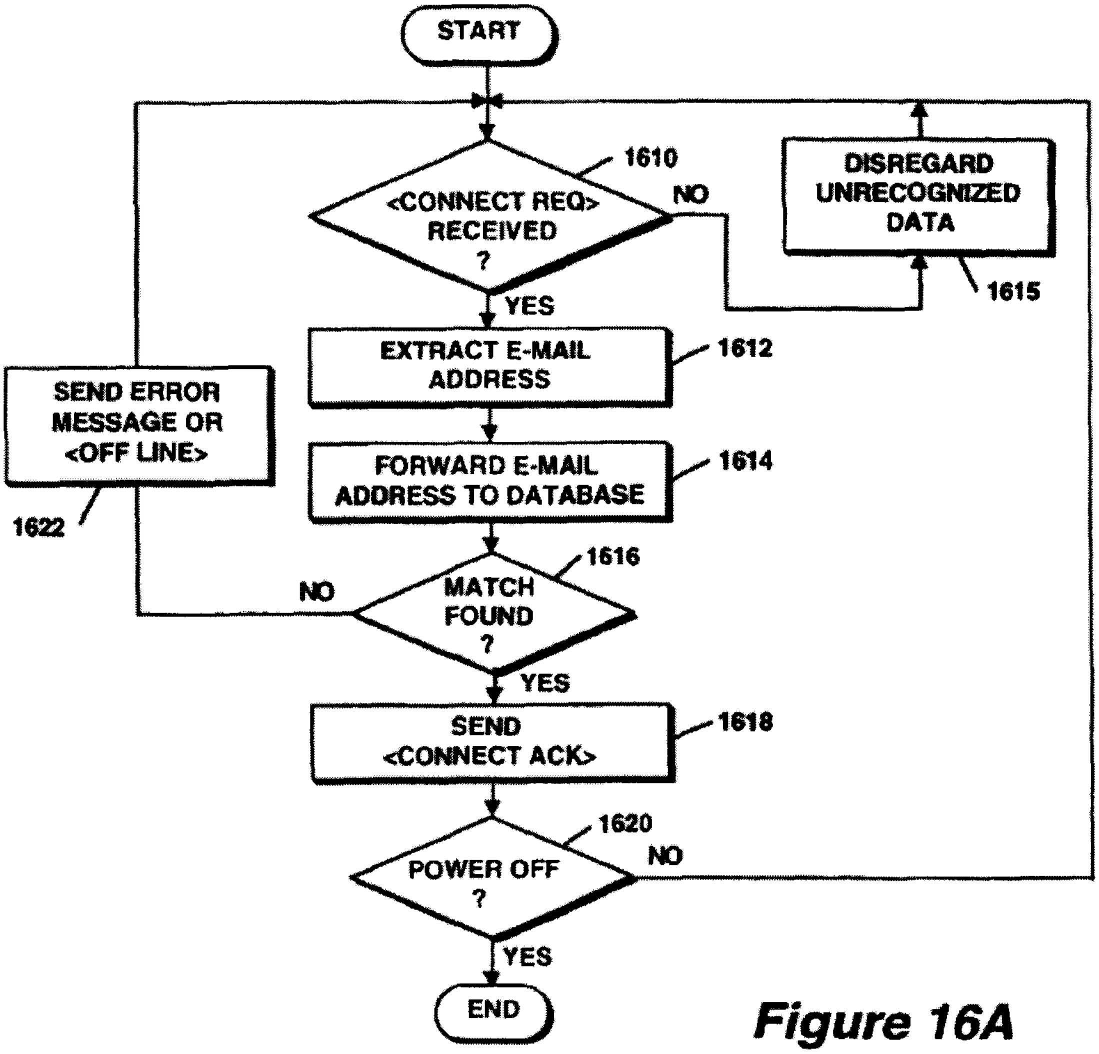


Figure 16A

Mattaway also describes a second protocol that involves sending messages via a mail server in order to implement the disclosed point-to-point communications protocol. For example:

> As described above, the first processing unit 12 may send the <ConnectReq> message in response to an unsuccessful attempt to perform the primary point-to-point Internet protocol. Alternatively, the first processing unit 12 may send the <ConnectReq> message in response to the first user initiating a SEND command or the like. After the <ConnectRequest> message via E-mail is sent, the first processing unit 12 opens a socket and waits to detect a response from the second processing unit 22. A timeout timer, such as timer 32, may be set by the first processing unit 12, in a manner known in the art, to wait for a predetermined duration to receive a <ConnectOK> signal. The processor 14 of the first processing unit 12 may cause 40 the output device 20 to output a Ring signal to the user, such as an audible ringing sound, about every 3 seconds. Mattaway at 8:25-44.

Thus, Mattaway discloses the step of "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device."

Step (d) of claim 26 further specifies: "sending a message securely from the first device to the second device."

Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34. Thus, Mattaway discloses the step of "sending a message securely from the first device to the second device."

Accordingly, Mattaway anticipates claim 26 of the '181 patent under 35 U.S.C. § 102(e).

21. Claim 27

Claim 27 depends from claim 26 and specifies:

(a) "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

(b) wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Step (a) of claim 27 further specifies: "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device."

Mattaway shows that the disclosed system and methods can include an unsecured name, such as a user's "alias." Mattaway at 11:13-15. The party's name may be stored in a "personal information directory" of other parties, Mattaway at 26:43-55, and "a party name field 1402A" will "display[] the name of the caller when an incoming call arrives," Mattaway at 26:45-47, and will when an outgoing call is made, so long as the party name has been stored in the directory. Mattaway at 26:63-67.

Thus, Mattaway discloses the step of "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device."

Step (b) of claim 27 further specifies: "wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Mattaway discloses a registration process in which the first processing unit registers a secure name associated with an IP address. For example:

> Upon the first user initiating the point-to-point Internet protocol when the first user is logged on to the Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server 26. The connection server 26 then stores these addresses in the database 34 . . . . Mattaway at 6:60-65.

Thus, Mattaway discloses the step of "wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Accordingly, Mattaway anticipates claim 27 of the '181 patent under 35 U.S.C. § 102(e).

22. Claim 28

Independent claim 28 is directed to "[a] non-transitory machine-readable medium comprising instructions for:

(a) sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

(b) receiving a message containing the network address associated with the secure name of the device; and

(c) sending a message to the network address associated with the secure name of the device using a secure communication link.

Accordingly, Mattaway anticipates claim 28 of the '181 patent under 35 U.S.C. § 102(e).

The preamble of claim 28 is directed to "[a] non-transitory machine-readable medium comprising constructions . . . ." Mattaway teaches, for example:

> a computer program product for use with a computer system compris[ing] a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client

> process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process form the server, and program code responsive to the network protocol address of the second client process for establishing a point-to-point communications link between the first client process and the second client process. Mattaway at 3:8-20.

Mattaway teaches a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20, as shown in Figure 1:

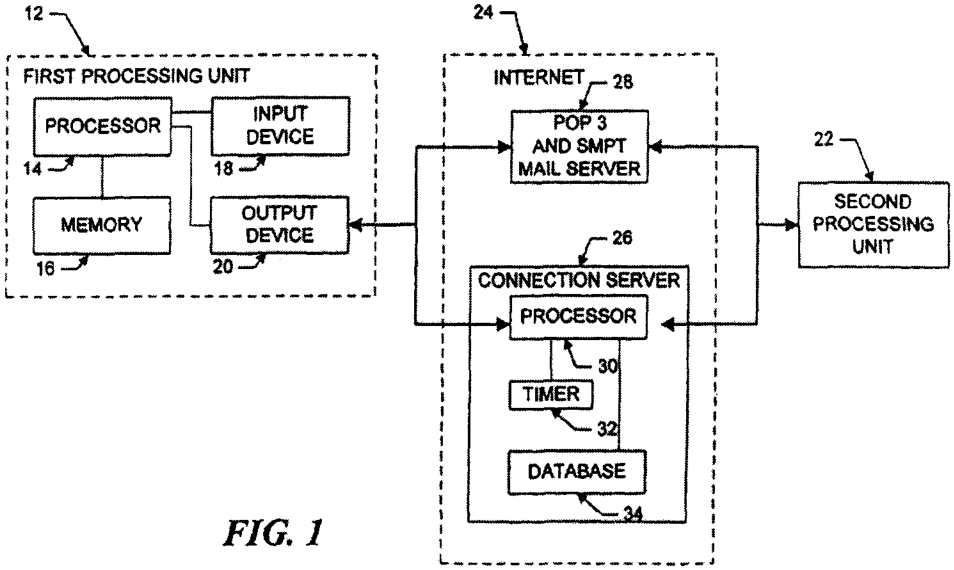


FIG. 1

Mattaway discloses that the first and second processing units (12, 22) may comprise VOIP ("Voice Over Internet Protocol") software that enable communications with other, for example, processing unites:

> In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, 40 Boca Raton, Fla., which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

Thus, Mattaway discloses "[a] non-transitory machine-readable medium comprising constructions."

Step (a) of claim 28 further specifies: "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

Mattaway shows that a first user must query the connection server in order to obtain the network address associated with the secure name of the second device. For example:

> The first processing unit 12 then sends a query, including the E-mail address of the callee, to the connection server 26. The connection server 26 then searches the database 34 to determine whether the callee is logged-in by finding any stored information corresponding to the callee's E-mail address indicating that the callee is active and on-line. If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. Mattaway at 7:24-37.

Thus, Mattaway discloses the step of "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

Step (b) of claim 28 further specifies: "receiving a message containing the network address associated with the secure name of the device."

Mattaway shows that the first device will receive a message from containing the network address associated with the secure name of the second device. For example:

> If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. Mattaway at 7:32-37.

Thus, Mattaway discloses the step of "receiving a message containing the network address associated with the secure name of the device."

Step (c) of claim 26 further specifies: "sending a message to the network address associated with the secure name of the device using a secure communication link."

Mattaway shows that the WebPhone application enables users who have established a connection via the disclosed point-to-point protocol to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34. Thus, Mattaway discloses the step of "sending a message to the network address associated with the secure name of the device using a secure communication link."

Accordingly, Mattaway anticipates claim 28 of the '181 patent under 35 U.S.C. § 102(e).

23. Claim 29

Independent claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

(a) receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and

(b) sending a message securely from the first device to the second device.

The preamble of claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name . . . ." Mattaway teaches, for example:

> a computer program product for use with a computer system compris[ing] a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process form the server, and program code responsive to the network protocol address of the second client process for establishing a point-to-point communications link between the first client process and the second client process. Mattaway at 3:8-20.

Mattaway teaches a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20, as shown in Figure 1:

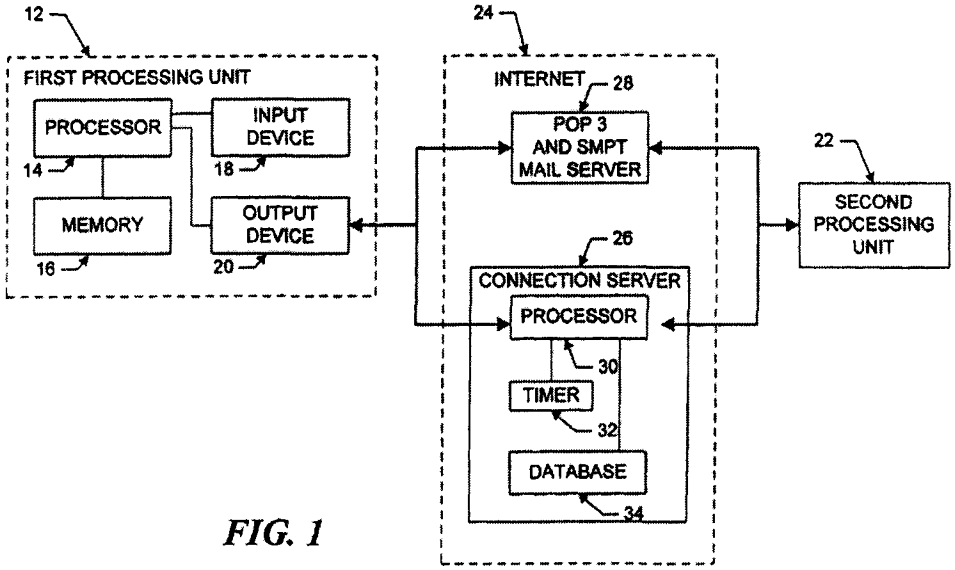


FIG. 1

Mattaway discloses that the first and second processing units (12, 22) may comprise VOIP ("Voice Over Internet Protocol") software that enable communications with other, for example, processing unites:

> In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, 40 Boca Raton, Fla., which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

Thus, Mattaway discloses "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name . . . ."

Step (a) of claim 29 further specifies: "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered."

Mattaway shows that the first device will receive a message from a second device of the desire to securely communicate. For example:

> If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e., the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. Mattaway at 7:32-37.

Mattaway describes two protocols for establishing point-to-point secure communications between two networked devices. The first protocol utilizes a connection server to implement a one-to-one mapping of E-mail addresses to Internet Protocol addresses." Mattaway at 18:41-45. The basic steps of this process are described in Figure 16A, which identifies the sending and receipt of a message of the intent to securely communicate. The receipt is represented by the <CONNECT ACK> packet, illustrated by decisional block 1616 and process block 1618:

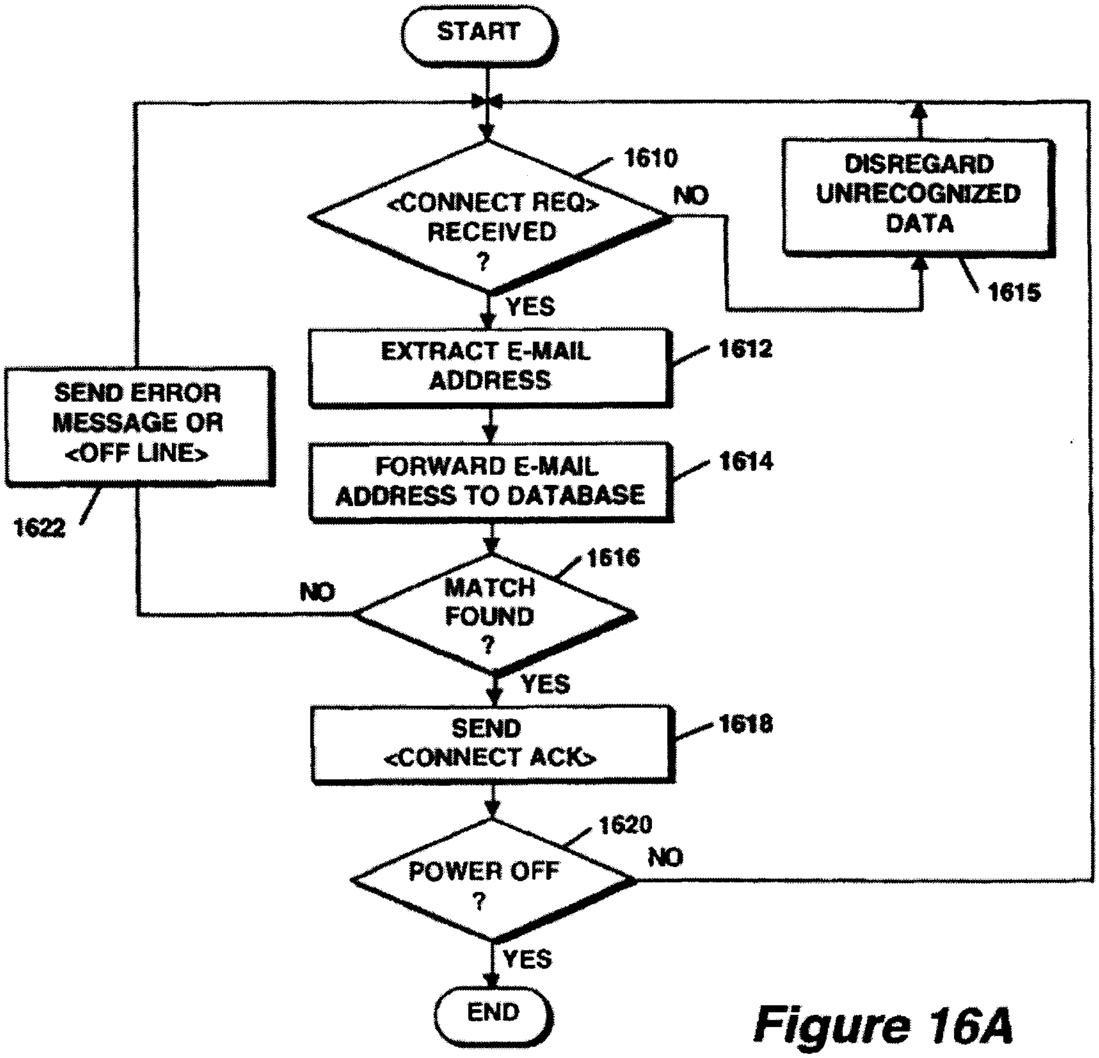


Figure 16A

Mattaway also describes a second protocol that involves sending messages via a mail server in order to implement the disclosed point-to-point communications protocol. For example:

> As described above, the first processing unit 12 may send the <ConnectReq> message in response to an unsuccessful attempt to perform the primary point-to-point Internet protocol. Alternatively, the first processing unit 12 may send the <ConnectReq>message in response to the first user initiating a SEND command or the like After the <ConnectRequest> message via E-mail is sent, the first processing unit 12 opens a socket and waits to detect a response from the second processing unit 22. A timeout timer, such as timer 32, may be set by the first processing unit 12, in a manner known in the art, to wait for a predetermined duration to receive a <ConnectOK> signal. The processor 14 of the first processing unit 12 may cause 40 the output device 20 to output a Ring

> signal to the user, such as an audible ringing sound, about every 3 seconds. Mattaway at 8:25-44.

Thus, Mattaway discloses the step of "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered."

Step (b) of claim 29 further specifies: "sending a message securely from the first device to the second device."

Mattaway shows that the WebPhone application enables users to engage in communications over a secure communication link: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Mattaway at 25:32-34. Thus, Mattaway discloses "sending a message securely from the first device to the second device."

Accordingly, Mattaway anticipates claim 29 of the '181 patent under 35 U.S.C. § 102(e).

D. Ground Nos. 4-5: Claims 3-4, 10-11, 18 and 23 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Mattaway in view of Beser and RFC 2401.

1. Relevant Teachings of the Primary Reference

A detailed explanation of how Mattaway anticipates claim 2 is provided in **§ V.A.**

2. Relevant Teachings of the Secondary References

a. Relevant Teachings of Beser

Beser generally describes methods and systems for establishing a secure communication link via a tunneling association in a data network. Beser explains that its method involves "negotiating private addresses, such as private Internet Address, for the ends of the tunneling association." *See* Beser, Abstract. Beser further explains that:

> The negotiation is performed on a public network, such as the Internet, through a trusted-third party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network. Beser, Abstract.

Beser explains that its methods involve a first and second network device, and a "trusted-third-party network device." According to Beser, the first and second network device "may be modified routers or modified gateways." Beser at 4:7-11. Beser further explains that in an exemplary preferred embodiment, the first or second network devices is an "edge router," which Beser explains "routes data packets between one or more networks such as a backbone network (e.g., a public network 12) and Local Area Networks (e.g., private network 20)." *Id.* at 4:19-24. An edge router is a computer, as it has a CPU, memory and storage.

Beser further explains that "the data network also includes network devices (24, 26) that are originating and terminating ends of data flow." *Id.* at 4:43-44. Beser indicates that these devices can include telephony and multimedia devices, and that data that is to be transmitted through the IP tunnels made by the Beser methods can include such telephony or multimedia applications. Beser at 4:47-50.

b. Relevant Teachings of RFC 2401

Generally, RFC 2401 is concerned with providing high quality security for Internet transactions that is adaptable to particular implementation needs and that facilitates interoperability over the Internet. *See, e.g.,* RFC 2401 at 4-5 ("The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations"; *see also Id.* at 5 ("A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.").

In particular, RFC 2401 defines the IPSec Protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes particular "cases" to implement secure communications involving a VPN, including "Case 3" which describes VPN implementation where edge routers on two different networks are used to establish an encrypted IP tunnel through which the network devices will communicate. RFC 2401 at 24-26.

3. Ground No. 4: Claims 3-4, 10-11, 18 and 23 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Mattaway in view of Beser.

a. Claim 3

Claim 3 depends from claim 2, and specifies "wherein the secure name of the second device is a secure domain name.

Beser teaches that the "secure name," i.e., the "unique identifier," can be a secure domain name. Beser at 10:38-41 ("In another exemplary preferred embodiment of the present invention, the unique identifier is any of a dial-up number, an electronic mail address, or a **domain name.**").

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of secure domain names disclosed by Beser would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 3 of the '181 patent under 35 U.S.C. § 103.

b. Claim 4

Claim 4 depends from claim 2, and specifies "wherein the secure name indicates security."

Mattaway recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, **encrypted audio communication** over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

The unique identifier disclosed in Beser is recognized by the trusted-third-party device as being secure and therefore implements protocols in order to obfuscate it from discovery by untrusted parties:

> For each transfer of a packet from the first network device 14 to the trusted-third-party network device 30, the first network device 14 constructs an IP 58 packet. . . . **The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12.** Beser at 11:13-25 (emphasis added).

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of secure names that indicate security as disclosed by Beser would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 4 of the '181 patent under 35 U.S.C. § 103.

c. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

Mattaway recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, **encrypted audio communication** over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by Beser would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 10 of the '181 patent under 35 U.S.C. § 103.

d. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

Mattaway recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, **encrypted audio communication** over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Beser shows that one of the security measures that can be performed by the disclosed methods "is that of initiating and maintaining a virtual tunnel." Beser at 6:58-59. Beser emphasizes the importance of protecting the negotiation process in order to protect from hackers the identities of the originating and terminating telephony devices:

> The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90 address fields of the IP 58 packets that comprise the negotiation. . . . In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26). Beser at 12:6-19.

Additionally, Beser teaches that when anonymity is required, encryption can be used:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. Beser at 2:6-12.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by Beser would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 11 of the '181 patent under 35 U.S.C. § 103.

e. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

Mattaway recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, **encrypted audio communication** over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Beser shows that it might be necessary to require authentication to conjunction with the secure communication link. Beser at 11:22-25 ("The IP 58 packets may require encryption or **authentication** to ensure that the unique identifier cannot be read on the public network 12.)

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of authentication by Beser would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 18 of the '181 patent under 35 U.S.C. § 103.

f. Claim 23

Claim 23 depends from claim 2 and specifies "wherein the secure name of the second device is a secure, non-standard domain name."

Beser teaches that the "secure name," i.e., the "unique identifier," can be a secure domain name, or in fact, other names which would not be resolvable by a DNS server. Beser at 10:38-41 ("In another exemplary preferred embodiment of the present invention, the unique identifier is any of a dial-up number, an electronic mail address, or a domain name.").

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of secure, non-standard domain names disclosed by Beser would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 23 of the '181 patent under 35 U.S.C. § 103.

4. Ground No. 5: Claims 10 and 11 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Mattaway in view of RFC 2401.

a. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

Mattaway recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, **encrypted audio communication** over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

Generally, RFC 2401 is concerned with providing high quality security for Internet transactions that is adaptable to particular implementation needs and that facilitates interoperability over the Internet. *See, e.g.*, RFC 2401 at 4-5 ("The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations"; *see also Id.* at 5 ("A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.").

In particular, RFC 2401 defines the IPSec Protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes particular "cases" to implement secure communications involving a VPN, including "Case 3" which describes VPN implementation where edge routers on two different networks are used to establish an encrypted IP tunnel through which the network devices will communicate. RFC 2401 at 24-26.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by RFC 2401 would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of RFC 2401 would render obvious claim 10 of the '181 patent under 35 U.S.C. § 103.

b. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

Generally, RFC 2401 is concerned with providing high quality security for Internet transactions that is adaptable to particular implementation needs and that facilitates interoperability over the Internet. *See, e.g.*, RFC 2401 at 4-5 ("The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations"; *see also Id.* at 5 ("A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.").

In particular, RFC 2401 defines the IPSec Protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes particular "cases" to implement secure communications involving a VPN, including "Case 3" which describes VPN implementation where edge routers on two different networks are used to establish an encrypted IP tunnel through which the network devices will communicate. RFC 2401 at 24-26.

Mattaway recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "[t]he Web Phone application enables the parties to converse in real-time, telephone quality, **encrypted audio communication** over the Internet and other TCP/IP based networks." Mattaway at 25:32-34.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by RFC 2401 would have been equally useful to those methods already described by Mattaway.

Accordingly, Mattaway in view of Beser would render obvious claim 11 of the '181 patent under 35 U.S.C. § 103.

VI. Detailed Explanation of Manner of Applying Lendenmann to Claims 1-29 and Proposed Rejections Based on Ground Nos. 6-8.

Exhibit C3 correlates each of claims 1-29 of the '181 patent with the section of the present request that sets out the detailed basis for anticipation and/or obviousness of the claim, along with an identification of the relevant portions of Lendenmann, alone and in conjunction with Beser, and RFC 2401. Requester notes that any emphasis indicated in quotations or other citations (e.g., as shown in bold faced text) has been added and is not original to the references cited in this section, unless otherwise noted.

A. Ground No. 6: Claims 1-9, 12-15, 18-29 are anticipated under 35 U.S.C. § 102(b) by Lendenmann

Lendenmann describes an implementation of the Open Software Foundation Distributed Computing Environment ("DCE"), which is a set of integrated services designed to support the development and use of distributed applications across a networked environment. The collection of machines, operating systems and networks, when managed by a single set of the disclosed DCE services is known as a DCE cell. The architecture is shown graphically below:

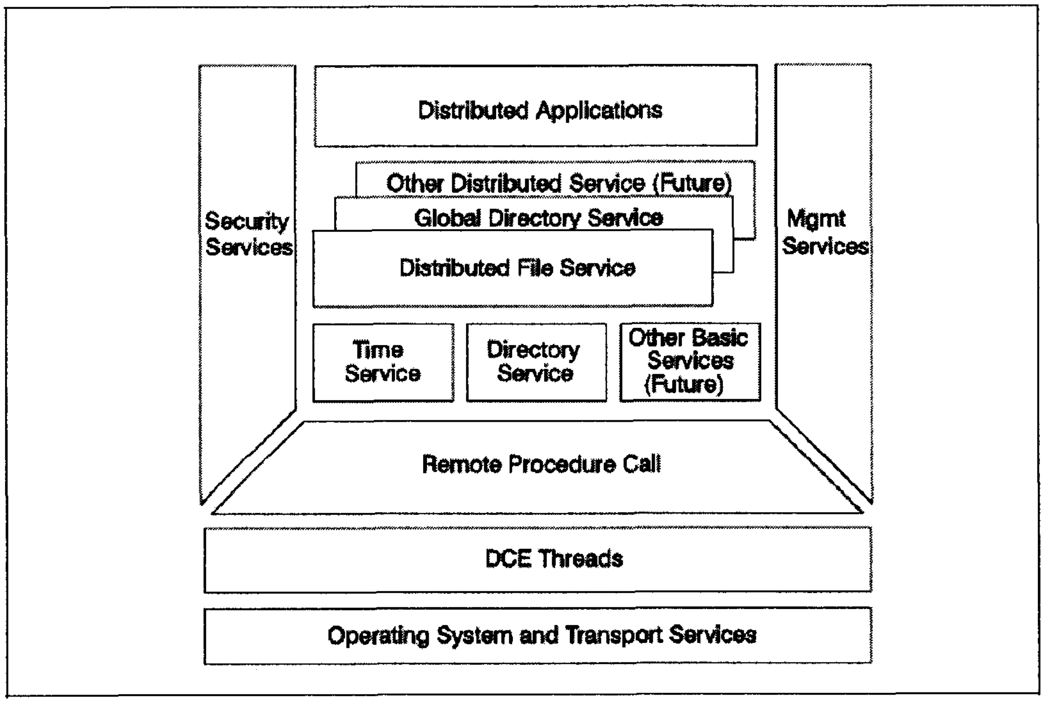


Figure 3. DCE Architecture

The software system described in Lendenmann provides a broad set of networking capabilities, including name resolution, security, and remote access features across a distributed network. For example, Lendenmann discloses naming services within DCE that provide name resolution for conventional public domain names and/or other unsecure names—such as Internet DNS or the CCITT X.500 naming scheme. Lendenmann additionally describes An exemplary comparison of the name representations disclosed in Lendenmann are shown in Figure 10:

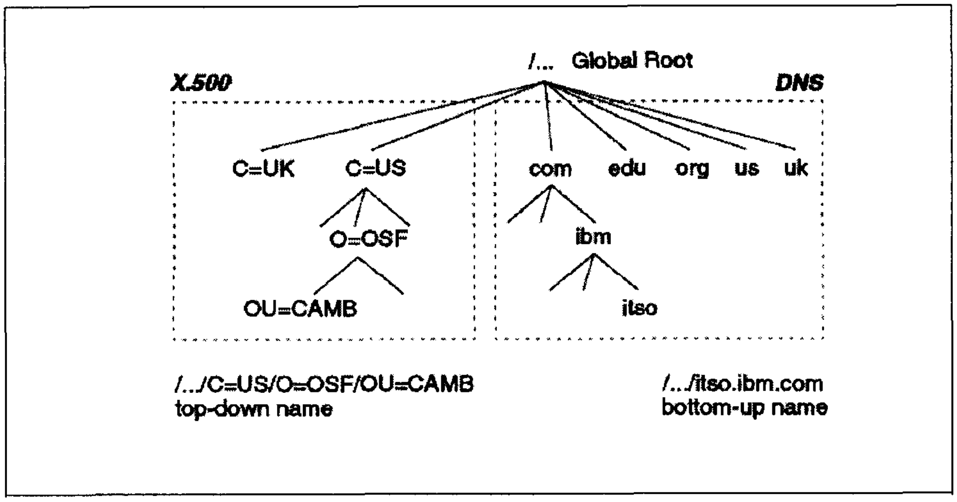


Figure 10. Comparison of Cell Name Representations

Lendenmann further teaches that users of its system are able to establish secure communications links within a cell in the DCE system utilizing the network address associated with the X.500 name, i.e., a secure name. Establishing such communications is through interaction with the directory and naming services disclosed and implementation of a remote procedure call ("RPC"), which provides the authenticated and encrypted communication between two devices.

In sum, Lendenmann discloses a system for securely communicating between two devices on a distributed network. The disclosed system utilizes secure and unsecured names in order to facilitate a secure communication link between two participating devices. Lendenmann thus provides a new and relevant disclosure in view of those references already considered by the Office.

1. Claim 1

Claim 1 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising":

(a) receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and

(b) sending a message over a secure communication link from the first device to the second device.

The preamble of claim 1 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name . . . ." The Open Software Foundation Distributed Computing Environment ("DCE") is a software system touting "a set of integrated services designed to support the development and use of distributed applications" in order to facilitate secure communications among devices within the DC. Lendenmann at 1. Each device within a DCE is associated with one or more secure and unsecured names. In a DCE, names can be assigned to each application, server, client, and/or machine. Multiple applications and/or servers can reside on a single machine, and the name of each machine, application, and server is contained in a DNS-type look-up service, called the Cell Directory Server ("CDS"). A query to the CDS using the disclosed application and/or devices results in the return of the IP address of the device and/or application queried. This collection of applications, servers, and/or services is referred to in OSF DCE as "network resources." Each DCE Cell is further represented in the Internet DNS system with an unsecured name.

In the DCE environment, a DCE Cell is a collection of machines that comprise a Security Server and a Cell Directory Server. For example:

> The collection of machines that are managed together as a DCE unit is referred to as a *cell*. At a minimum, a cell must contain a Security Server, a Cell Directory Server and Distributed Time Servers. All of these services may run on one machine, or the servers can be spread among the machines that are to be part of the cell. The Directory, Time and Security Services are collectively known as the core services. Lendenmann at 9.

DCE Directory Services allow users to identify, by name, network resources for access using either a DNS name or a CCITT X.500 name:

> The Directory Service provides a naming model throughout the distributed environment that allows users to identify, by name, network resources, such as servers, users, files, disks, or print queues. The DCE Directory Service includes:
>
> - Cell Directory Service (CDS)
> - Global Directory Service (GDS)
> - Global Directory Agent (GDA)
> - Application Programming Interface (API)
>
> The CDS manages information within a cell. The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

The client-server architecture described in Lendenmann is not limited to a traditional client-server understanding. Instead, the disclosed system contemplates that a single device is able to play the role of both client and server. Lendenmann discloses, for example:

> The terms client and server can refer to the role of a single application. For example, machine A may have a program that requests a piece of information from another machine, B. In this example, the program running on machine A is assuming the role of a client, while the program on machine B that fulfills the request is acting as the server. It is not hard to imagine that in a multitasking operating system environment we may have both client and server applications running on the same machine at the same time. It is also not hard to see that both the client and server functions for a transaction may both run on the same machine. In many cases, it will be necessary for the machine running the server to also run the client application in order to obtain access to the function it is serving. Lendenmann at 8-9.

The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. Lendenmann teaches secure names as follows:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations.
>
> CDS authorization allows you to control user access to:
>
> - ***Names in the namespace***, including clearinghouses, directories, object entries, soft links, and child pointers
>
> - Execution of privileged CDS clerk and server commands
>
> Access control is done by creating access control lists (ACL) that contain individual ACL entries that determine which user (principal) ***can use the name*** and what management operations they are allowed to perform on it.
>
> CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests. When a principal requests an operation on a CDS name or a privileged operation on a CDS clerk or server, ACL management software examines the ACL entry associated with that name or principal name and grants or denies the operation. Lendenmann at 34 (emphasis added).

Lendenmann also teaches that the CDS is a secure name service. *See id.* and the following:

> The directory service component that controls names inside a cell is called the Cell Directory Service (CDS). The CDS stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource. Lendenmann at 21.

Lendenmann also enables users to identify and access foreign cells over the Internet utilizing an unsecure name, e.g., the public DNS. Lendenmann at 23. For example, when a client within a particular DCE cell desires to communicate with the host in different DCE cell—presumably across the Internet—the client may utilize the disclosed DNS system in order to obtain the IP address of the CDS in the different cell. *See, e.g.,* Lendenmann at 131-32 (setting up intercell communication by registering an MX record in the public DNS system that identifies the CDS in the foreign network). After obtaining the IP address of the "foreign" CDS server, the client queries the foreign CDS server for the IP address of the desired host in the "foreign" network. The CDS then returns the IP address of the desired host in the foreign cell to the requesting client. The DNS record in the public DNS is thus an unsecured name associated with the foreign cell, i.e., is associated with all hosts in the foreign cell. Lendenmann at 8-10, 23. In other words, Lendenmann teaches that each host within a cell is associated with a cell name that is registered in the public DNS that identifies the CDS containing the IP address of that host.

The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.
>
> There are two well-established naming schemes in place that DCE makes use of:
>
> - CCITT X.500
> - Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

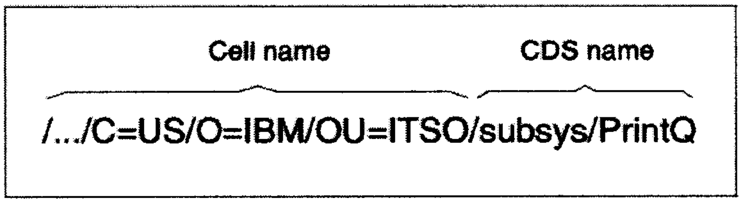


Figure 9. Global Representation of a Subsystem Printer Queue

Further, the distinction between the X.500 and DNS naming conventions can be distilled, for example, from the Figure 10 in Lendenmann:

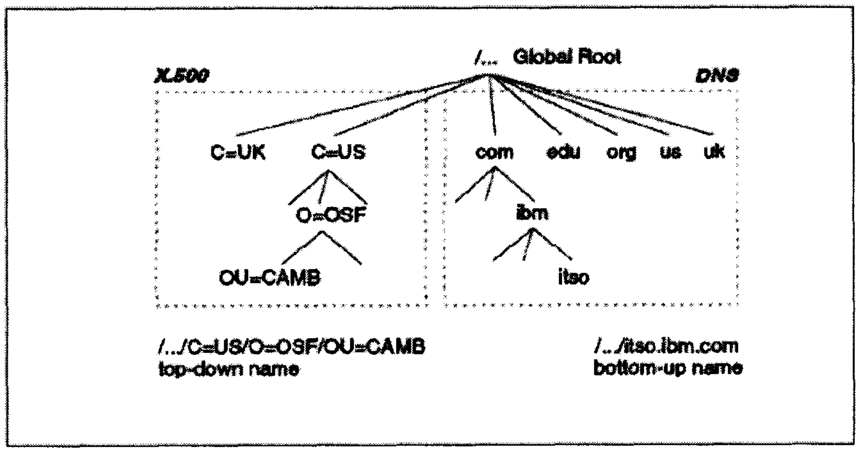


Figure 10. Comparison of Cell Name Representations

Lendenmann shows that a given device in the DCE system is able to have multiple names through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Thus, Lendenmann discloses "a non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name."

Step (a) of Claim 1 specifies: "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and"

Lendenmann discloses that devices in DCE—and the distributed client/server applications within—"use remote procedure calls (RPCs) to make function calls (transparently) across a network." Lendenmann at 173. Establishing a relationship in the DCE client/server model requires a "binding" between the client and server. "A binding is a temporary relationship that depends on a communications link." Lendenmann at 174. RPC Runtime, which is a component involved in the processing of an RPC, is responsible for "perform[ing] such tasks as controlling communication between clients and servers or finding servers for the clients on request."

RPC Runtime provides a number of different services. For example, RPC Runtime "is responsible for establishing a binding (the communication link) and for the data transfer between client and server." Lendenmann at 178. RPC is also responsible for providing "Directory service interface operations." Lendenmann at 178. The Directory Service described in

Lendenmann enables users to find other networked objects without knowing their physical location.

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information." Lendenmann at 178-79.

One of the many ways a second device can locate a network address of a first device is through the CDS:

> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a *binding*.... A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the *Name Service Interface* import operations. Lendenmann at 182.

The steps involved in locating the address of another device in represented graphically in Lendenmann in Figure 68:

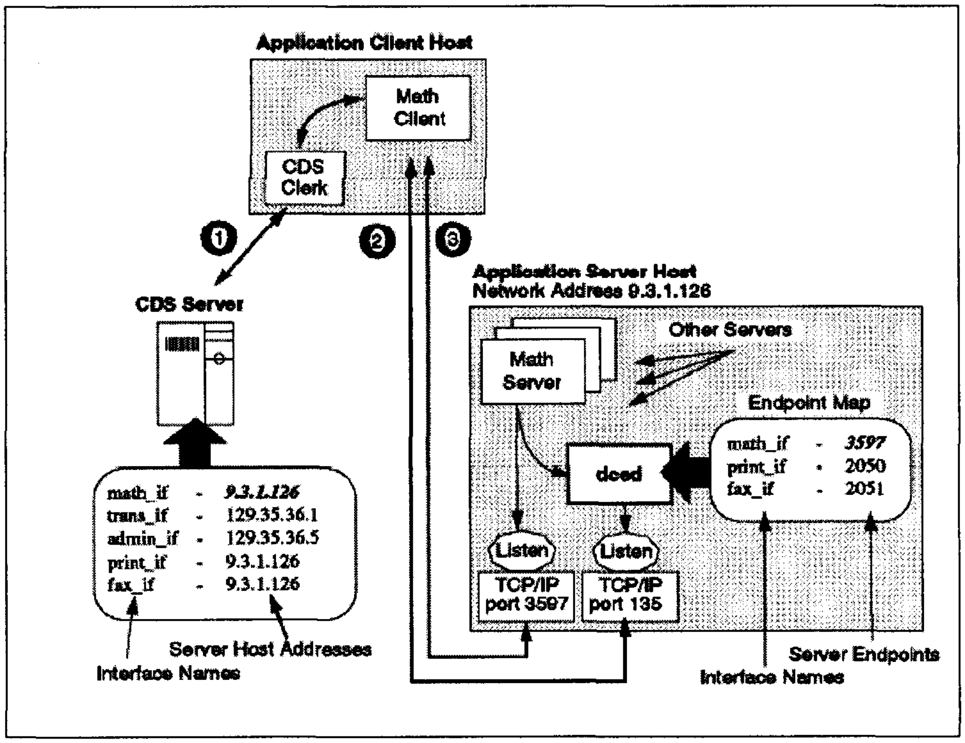


Figure 68. Steps Involved in Finding a Server

The first step in the process, as shown in Figure 68, is looking up the network address information of the server/device that the client/device is seeking to communicate. Once the network is address is known, the client/device's "RPC runtime then directly calls the server process listening to the endpoint." Lendenmann at 191.

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Thus, Lendenmann discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Step (b) of claim 1 specifies: "sending a message over a secure communication link from the first device to the second device."

As discussed above in **Step (a),** Lendenmann permits users of the system to define the level of security a client/device wants to establish when communicating with another device. Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

- None. No communication protection.
- Connection. Performs an encrypted handshake the first time the client communicates with the server.
- Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
- Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
- Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.

- CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.
- Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Thus, Lendenmann discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Lendenmann anticipates claim 1 of the '181 patent under 35 U.S.C. § 102(b).

2. Claim 2

Independent claim 2 is directed to [a] method of using a first device to communicate with a second device having a secure name, the method comprising:

(a) from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;

(b) at the first device, receiving a message containing the network address associated with the secure name of the second device; and

(c) from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

The preamble of claim 2 specifies "[a] method of using a first device to communicate with a second device having a secure name . . . ." The Open Software Foundation Distributed Computing Environment ("DCE") is a software system touting "a set of integrated services designed to support the development and use of distributed applications" in order to facilitate secure communications among devices within the DC. Lendenmann at 1. Each device within a DCE is associated with one or more secure and unsecured names. In a DCE, names can be assigned to each application, server, client, and/or machine. Multiple applications and/or servers can reside on a single machine, and the name of each machine, application, and server is contained in a DNS-type look-up service, called the Cell Directory Server ("CDS"). A query to the CDS using the disclosed application and/or devices results in the return of the IP address of the device and/or application queried. This collection of applications, servers, and/or services is referred to in OSF DCE as "network resources." Each DCE Cell is further represented in the Internet DNS system with an unsecured name.

In the DCE environment, a DCE Cell is a collection of machines that comprise a Security Server and a Cell Directory Server. For example:

> The collection of machines that are managed together as a DCE unit is referred to as a *cell.* At a minimum, a cell must contain a Security Server, a Cell Directory Server and Distributed Time Servers. All of these services may run on one machine, or the servers can be spread among the machines that are

> to be part of the cell. The Directory, Time and Security Services are collectively known as the core services. Lendenmann at 9.

DCE Directory Services allow users to identify, by name, network resources for access using either a DNS name or a CCITT X.500 name:

> The Directory Service provides a naming model throughout the distributed environment that allows users to identify, by name, network resources, such as servers, users, files, disks, or print queues. The DCE Directory Service includes:
>
> - Cell Directory Service (CDS)
> - Global Directory Service (GDS)
> - Global Directory Agent (GDA)
> - Application Programming Interface (API)
>
> The CDS manages information within a cell. The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

When a client within a particular DCE cell desires to communicate with the host in different DCE cell—presumably across the Internet—the client may utilize the disclosed DNS system in order to obtain the IP address of the CDS in the different cell. After obtaining the IP address of the "foreign" CDS server, the client queries the foreign CDS server for the IP address of the desired host in the "foreign" network. The local CDS then returns the IP address of the desired host in the foreign cell to the requesting client. The DNS record in the public DNS is thus an unsecured name associated with the foreign cell, i.e., is associated with all hosts in the foreign cell. Lendenmann at 8-10, 23.

The client-server architecture described in Lendenmann is not limited to a traditional client-server understanding. Instead, the disclosed system contemplates that a single device is able to play the role of both client and server. Lendenmann discloses, for example:

> The terms client and server can refer to the role of a single application. For example, machine A may have a program that requests a piece of information from another machine, B. In this example, the program running on machine A is assuming the role of a client, while the program on machine B that fulfills the request is acting as the server. It is not hard to imagine that in a multitasking operating system environment we may have both client and server applications running on the same machine at the same time. It is also not hard to see that both the client and server functions for a transaction may

> both run on the same machine. In many cases, it will be necessary for the machine running the server to also run the client application in order to obtain access to the function it is serving. Lendenmann at 8-9.

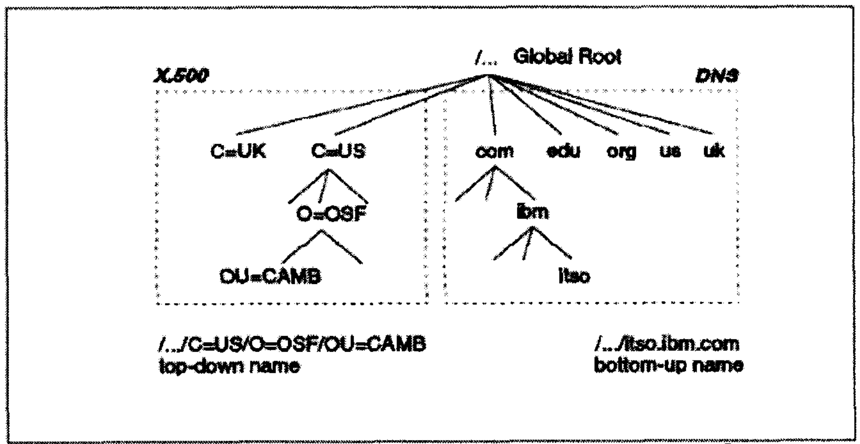
The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. It also enables users to identify and access foreign cells over the Internet utilizing an unsecure name. Lendenmann at 23. The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.
>
> There are two well-established naming schemes in place that DCE makes use of:
>
> - CCITT X.500
> - Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

Further, the distinction between the X.500 and DNS naming conventions can be distilled, for example, from the Figure 10 in Lendenmann:

Lendenmann shows that a given device in the DCE system is able to have multiple names through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the



primary name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Thus, Lendenmann discloses "[a] method of using a first device to communicate with a second device having a secure name."

Step (a) of claim 2 further specifies: "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Lendenmann discloses that devices in DCE—and the distributed client/server applications within—"use remote procedure calls (RPCs) to make function calls (transparently) across a network." Lendenmann at 173. Establishing a relationship in the DCE client/server model requires a "binding" between the client and server. "A binding is a temporary relationship that depends on a communications link." Lendenmann at 174. RPC Runtime, which is a component involved in the processing of an RPC, is responsible for "perform[ing] such tasks as controlling communication between clients and servers or finding servers for the clients on request."

RPC Runtime provides a number of different services. For example, RPC Runtime "is responsible for establishing a binding (the communication link) and for the data transfer between client and server." Lendenmann at 178. RPC is also responsible for providing "Directory service interface operations." Lendenmann at 178. The Directory Service described in Lendenmann enables users to find other networked objects without knowing their physical location. Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information." Lendenmann at 178-79.

One of the many ways a second device can locate a network address of a first device is through the CDS:

> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a *binding*.... A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the *Name Service Interface* import operations. Lendenmann at 182.

The CDS is a secure name service; it controls access to the namespace:

> 2.5 Security in CDS Environment

> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations.
>
> CDS authorization allows you to control user access to:
>
> - ***Names in the namespace***, including clearinghouses, directories, object entries, soft links, and child pointers
>
> - Execution of privileged CDS clerk and server commands
>
> Access control is done by creating access control lists (ACL) that contain individual ACL entries that determine which user (principal) ***can use the name*** and what management operations they are allowed to perform on it.
>
> CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests. When a principal requests an operation on a CDS name or a privileged operation on a CDS clerk or server, ACL management software examines the ACL entry associated with that name or principal name and grants or denies the operation. Lendenmann at 34 (emphasis added).

And:

> The directory service component that controls names inside a cell is called the Cell Directory Service (CDS). The CDS stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource. Lendenmann at 21.

Thus, Lendenmann shows the step of "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Step (b) of claim 2 further specifies: "at the first device, receiving a message containing the network address associated with the secure name of the second device; and"

Lendenmann discloses the steps involved in retrieving the address of another device graphically in Figure 68:

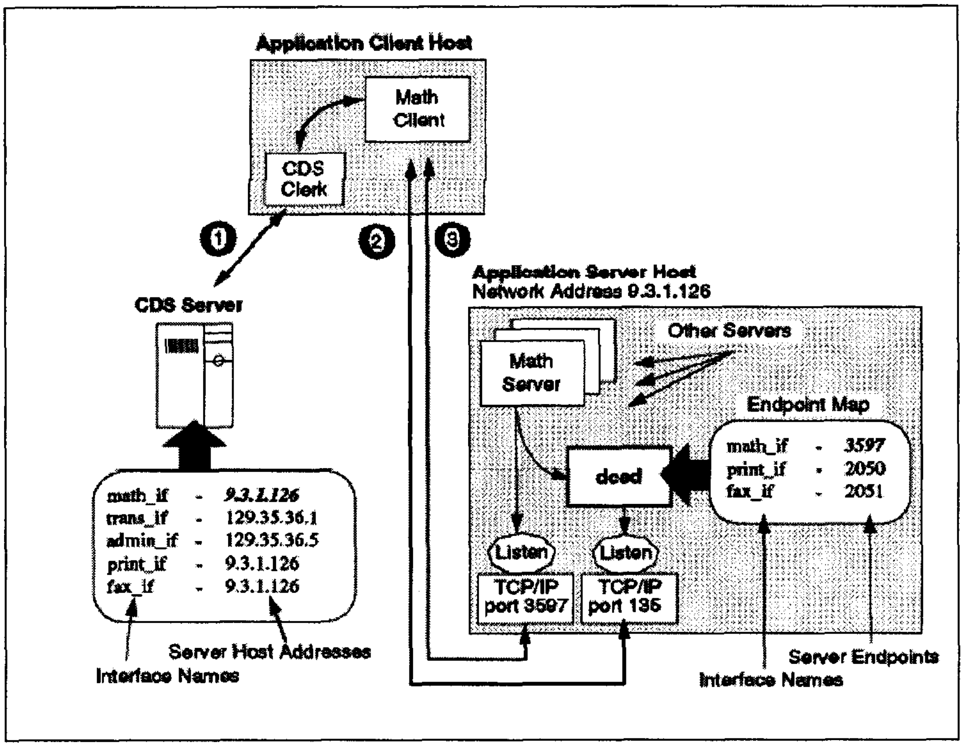


Figure 68. Steps Involved in Finding a Server

The first step in the process, as shown in Figure 68, is looking up the network address information of the server/device that the client/device is seeking to communicate. Once the network is address is known, the client/device's RPC runtime—using the network address information provided by the CDS—"then directly calls the server process listening to the endpoint." Lendenmann at 191.

Thus, Lendenmann shows the step of "at the first device, receiving a message containing the network address associated with the secure name of the second device."

Step (c) of claim 2 further specifies: "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

- None. No communication protection.
- Connection. Performs an encrypted handshake the first time the client communicates with the server.
- Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
- Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
- Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
- CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.
- Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Thus, Lendenmann shows the step of "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

Accordingly, Lendenmann anticipates claim 2 of the '181 patent under 35 U.S.C. § 102(b).

3. Claim 3

Claim 3 depends from claim 2, and specifies "wherein the secure name of the second device is a secure domain name.

Figure 11, at Lendenmann at 24, shows cell names comprise domain names:

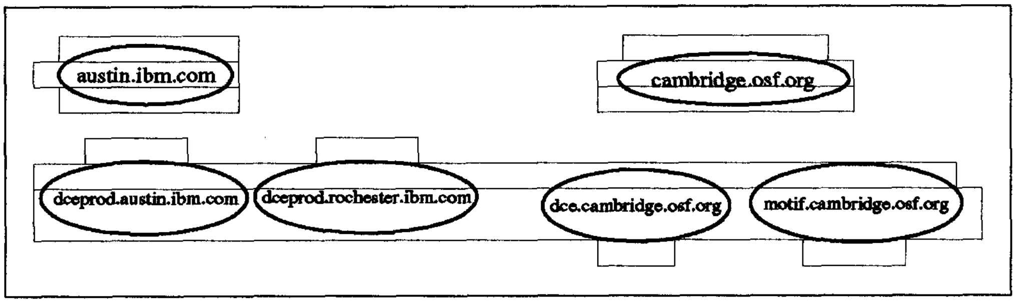


Figure 11. Related Cells

Figure 11 shows DCE cells that may have grown independently from each other. They may have set up intercell communication individually and exported their names into DNS (or GDS if the cell names were X.500). These cells may now be integrated into hierarchical structures within their companies with only the top-most cell names exported into DNS.

DCE naming includes a domain name portion:

2.3.6 Summary: DCE Naming

Let us summarize the naming convention with an example of a file in a Distributed File System (DFS). The file name is local/bin/ghostscript, a tool used to view postscript files. We want to make this available in the shared file system of the DCE cell itso.austin.ibm.com.

Users within the itso.austin.ibm.com cell execute this command in one of the following ways:

- /:/local/bin/ghostscript
- /.:/fs/local/bin/ghostscript
- /.../itso.austin.ibm.com/fs/local/bin/ghostscript

Of course, they would normally use the first option. Users of other cells would find this file only by specifying the third command:

- /.../itso.austin.ibm.com/fs/local/bin/ghostscript

This is DNS naming. If the cell had been defined with X.500 syntax, the global access could only be established with the following command:

- /.../C=US/O=IBM/OU=ITSO/CN=AUSTIN/fs/local/bin/ghostscript

Lendenmann at 28.

Cell names are names of domains.

The CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the

$$\overbrace{\text{/.../C=US/O=IBM/OU=ITSO}}^{\text{Cell name}}\overbrace{\text{/subsys/PrintQ}}^{\text{CDS name}}$$

Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

Lendenmann describes the components of the secure domain name represented by the X.500 naming scheme:

> Figure 9 shows a global name that refers to a printer queue object defined in the IBM ITSO cell. Local users can address it with /.:/susbsys/PrintQ. The prefix (/...) indicates that the name is global. Following the prefix, the X.500 syntax defines four blocks, each one with two parts separated by an equal sign (=). The abbreviation of each block stands for country (C), organization (O), organizational unit (OU), and common name (CN, not shown). Lendenmann at 23.

Accordingly, Lendenmann anticipates claim 3 of the '181 patent under 35 U.S.C. § 102(b).

4. Claim 4

Claim 4 depends from claim 2, and specifies "wherein the secure name indicates security."

Lendenmann shows that the DCE components GDS and GDA are designed to detect both traditional addresses and those related to the CCITT X.500 secure name scheme. For example:

> The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

Accordingly, Lendenmann anticipates claim 4 of the '181 patent under 35 U.S.C. § 102(b).

5. Claim 5

Claim 5 of the '181 patent depends from claim 2, and specifies "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form."

Lendenmann discloses that the CDS, from which the network address associated with the secure name of a second device is obtained, is integrated into the security services featured in the DCE system. For example:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations. Lendenmann at 34.

A significant part of the authentication concepts of the DCE Security Service described in Lendenmann "are keys and tickets. Keys are used to encrypt/decrypt messages." Lendenmann at 57.

Querying the CDS for a server address requires using the CDS Name Service Interface (NSI) import operations:

> 10.3 Finding Remote Services
>
> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a binding. There are several ways in which a client can find a server. The most simple is to hard-code the address, endpoint and protocols of a server into the application. Obviously this implementation is not flexible. A more flexible way is to use the namespace maintained by the Cell Directory Service. A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the Name Service Interface [NSI] import operations. Lendenmann at 182.

NSI utilizes RPC routines:

> 10.3.2.2 Searching The Namespace
>
> NSI provides two methods for finding a server, the rpc_ns_binding_import_*() routines and the rpc_ns_binding_lookup_*() routines. Both operations search server entries for a compatible server. Lendenmann at 186.

RPC routines include specifying a protection level to be used:

> 10.4 RPC and Security
>
> DCE RPC supports authenticated communications between clients and servers [including the CDS]. Authenticated RPC is provided by the RPC runtime facility and works with the authentication and authorization services provided by the DCE security service.
>
> Before authenticated RPC can be used, the application server registers its principal name and the supported authentication service with its RPC runtime. A server usually assumes its own (authenticated) login identity during its initialization. It performs the equivalent of a user login by specifying its DCE account name and password stored in the local keytab file. See also 10.5.6, "Developing a Basic Server" on page 199 for details on the server initialization steps.

> A client usually runs with the login context of the user that called it. To use authenticated RPC, a client must specify the server principal name and establish the authentication service, ***protection level*** and authorization service that it wants to use in its communications with a server. The client does this with a call to rpc_binding_set_auth_info(), which adds this security information to the server binding handle. The client then uses this extended binding handle in its further RPC calls. Lendenmann at 192.

The CDS is a server in DCE:

> Each cell is a self-sufficient, independently managed unit in a global distributed computing environment. It must at least have the following DCE core services:
>
> • One Security Server
>
> • ***One CDS Server***
>
> • Three DTS Servers per LAN (the use of DTS is optional). Lendenmann at 21 (emphasis added).

The protection level determines the degree to which client/server messages are encrypted:

> 10.4.2 Level of Protection
>
> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Accordingly, Lendenmann anticipates claim 5 of the '181 patent under 35 U.S.C. § 102(b).

6. Claim 6

Claim 6 depends from claim 2, and specifies that the step of "further including decrypting the message."

Lendenmann discloses that the CDS, from which the network address associated with the secure name of a second device is obtained, is integrated into the security services featured in the DCE system. For example:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations. Lendenmann at 34.

Querying the CDS for a server address requires using the CDS Name Service Interface (NSI) import operations:

> 10.3 Finding Remote Services
>
> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a binding. There are several ways in which a client can find a server. The most simple is to hard-code the address, endpoint and protocols of a server into the application. Obviously this implementation is not flexible. A more flexible way is to use the namespace maintained by the Cell Directory Service. A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the Name Service Interface [NSI] import operations. Lendenmann at 182.

NSI utilizes RPC routines:

> 10.3.2.2 Searching The Namespace
>
> NSI provides two methods for finding a server, the rpc_ns_binding_import_*() routines and the rpc_ns_binding_lookup_*() routines. Both operations search server entries for a compatible server. Lendenmann at 186.

RPC routines include specifying a protection level to be used:

> 10.4 RPC and Security
>
> DCE RPC supports authenticated communications between clients and servers [including the CDS]. Authenticated RPC is provided by the RPC runtime facility and works with the authentication and authorization services provided by the DCE security service.
>
> Before authenticated RPC can be used, the application server registers its principal name and the supported authentication service with its RPC runtime. A server usually assumes its own (authenticated) login identity during its initialization. It performs the equivalent of a user login by specifying its DCE account name and password stored in the local keytab file. See also 10.5.6, "Developing a Basic Server" on page 199 for details on the server initialization steps.
>
> A client usually runs with the login context of the user that called it. To use authenticated RPC, a client must specify the server principal name and establish the authentication service, ***protection level*** and authorization service that it wants to use in its communications with a server. The client does this with a call to rpc_binding_set_auth_info(), which adds this security information to the server binding handle. The client then uses this extended binding handle in its further RPC calls. Lendenmann at 192.

The CDS is a server in DCE:

> Each cell is a self-sufficient, independently managed unit in a global distributed computing environment. It must at least have the following DCE core services:
>
> • One Security Server
>
> • ***One CDS Server***
>
> • Three DTS Servers per LAN (the use of DTS is optional). Lendenmann at 21 (emphasis added).

The protection level determines the degree to which client/server messages are encrypted:

> 10.4.2 Level of Protection
>
> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

A significant part of the authentication concepts of the DCE Security Service described in Lendenmann "are keys and tickets. Keys are used to encrypt/decrypt messages." Lendenmann at 57.

Accordingly, Lendenmann anticipates claim 6 of the '181 patent under 35 U.S.C. § 102(b).

7. Claim 7

Claim 7 of the '181 patent depends from claim 2, and specifies "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed."

Lendenmann details some of the different protection levels that are available in establishing communications with other devices:

- None. No communication protection.
- Connection. Performs an encrypted handshake the first time the client communicates with the server.
- Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
- Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
- Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
- CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.

- Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Accordingly, Lendenmann anticipates claim 7 of the '181 patent under 35 U.S.C. § 102(b).

8. Claim 8

Claim 8 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

Lendenmann discloses that the secure name of a device is associated with an IP address. For example, Figure 66 illustrates that the CDS server shows that an IP address is associated with the secure name and is what is transmitted in the message:

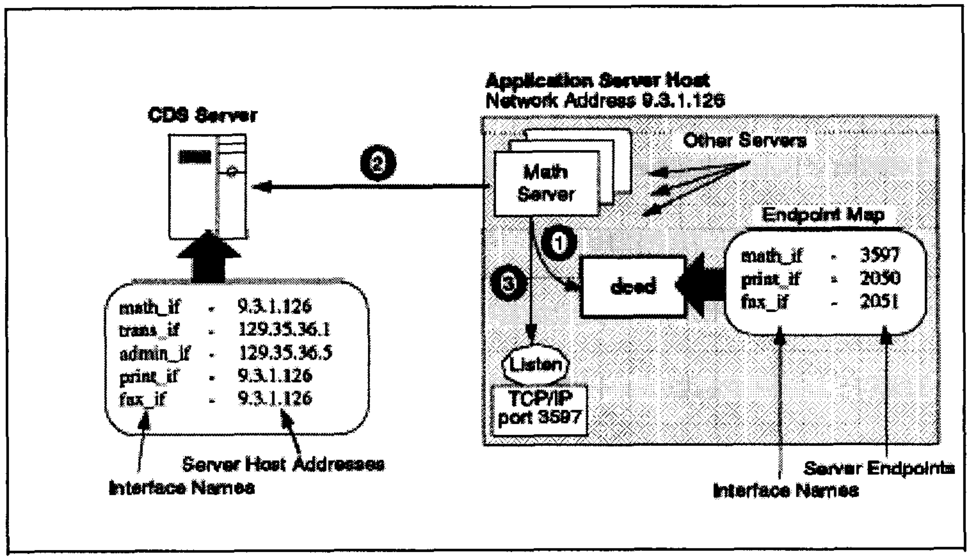


Figure 66. Server Initialization

Lendenmann at 181.

Accordingly, Lendenmann anticipates claim 8 of the '181 patent under 35 U.S.C. § 102(b).

9. Claim 9

Claim 9 depends from claim 2 and specifies that "further including automatically initiating the secure communication link after it is enabled."

Lendenmann shows that after the user selects the level of security, the secure communication link is automatically initiated. Lendenmann at 9.

Accordingly, Lendenmann anticipates claim 9 of the '181 patent under 35 U.S.C. § 102(b).

10. Claim 12

Claim 12 depends from claim 2 and specifies "wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols."

Apart from utilizing Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Protocol (IP), Lendenmann at 179-80, DCE additionally implements the following protocols, for example:

> An RPC protocol is a communication protocol that supports the semantics of DCE RPC API and is responsible for marshaling and unmarshaling. It runs over specific combinations of transport and network protocols. DCE RPC provides two RPC protocols:
>
> 1. Network Computing Architecture Connection-Based Protocol (NCACN)
>
> This protocol runs over a connection-oriented transport protocol, such as TCP. It guarantees reliability in the delivery of data, and it provides indication of a connection loss.
>
> 2. Network Computing Architecture Datagram Protocol (NCADG)
>
> This connectionless protocol runs over connectionless transport protocols, such as UDP. DG does it "as best as it can". Packets are individually addressed. They can follow different network paths; therefore, the sequence of the incoming packets may be mixed up. Packets can get lost. Reliability must be provided by higher layers; it is not protocol-inherent. DG protocol supports broadcast calls. Lendenmann at 179.

Accordingly, Lendenmann anticipates claim 12 of the '181 patent under 35 U.S.C. § 102(b).

11. Claim 13

Claim 13 depends from claim 2 and specifies "wherein the receiving and sending of messages through the secure communication link includes multiple sessions."

Lendenmann shows that a system that implements the DCE system utilizing RPC's can perform a number of tasks through the secure communications link through multiple sessions. For example:

> Although RPCs are synchronous, the use of multiple threads of execution allows the client to perform other tasks while one thread is waiting for an RPC to terminate. This does not change the synchronous behavior of RPCs, but

> gives some of the benefits of asynchronous models to the client application. Lendenmann at 176.

Servers handle multiple requests:

> - Multithreaded servers — DFS servers make use of DCE threads support to efficiently handle multiple file requests from the clients. Lendenmann at 100.

Accordingly, Lendenmann anticipates claim 13 of the '181 patent under 35 U.S.C. § 102(b).

12. Claim 14

Claim 14 depends from claim 2 and specifies "further including supporting a plurality of services over the secure communication link."

Lendenmann discloses a number of services supported by the DCE RPC Runtime. For example:

> - Communication operations
>
> The RPC runtime is responsible for establishing a binding (the communication link) and for the data transfer between client and server. At initialization, RPC servers makes a number of calls to communications operations, for example, for selecting the protocol sequences to be used.
>
> - Directory service interface operations
>
> The RPC runtime can be used to store and search for the location of servers (binding information) in the directory service (CDS). The CDS can be accessed through DCE RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information.
>
> - Endpoint operations
>
> On one host, there could be several RPC servers running; so a host address is not sufficient to locate a server. The complete address of a server instance is called a fully bound binding handle, and it contains a host address and an endpoint (see 10.3.1, "Binding Handles" on page 182). DCE RPC endpoint operations allow servers to dynamically create their own endpoints in the local endpoint map. Clients can resolve partial binding information into fully bound binding handles that contain the appropriate endpoints.
>
> - Authentication operations

> The authentication operations prove the identity of clients and servers to each other in order to make appropriate authorization decisions. The RPC authentication operations define what authentication mechanism (usually DCE Kerberos) and what protection level will be used for ongoing RPC communication. Lendenmann at 178-79.

Accordingly, Lendenmann anticipates claim 14 of the '181 patent under 35 U.S.C. § 102(b).

13. Claim 15

Claim 15 depends from claim 14 and specifies "wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof."

Apart from utilizing Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Protocol (IP), Lendenmann at 179-80, DCE additionally implements the following protocols, for example:

> An RPC protocol is a communication protocol that supports the semantics of DCE RPC API and is responsible for marshaling and unmarshaling. It runs over specific combinations of transport and network protocols. DCE RPC provides two RPC protocols:
>
> 1. Network Computing Architecture Connection-Based Protocol (NCACN)
>
> This protocol runs over a connection-oriented transport protocol, such as TCP. It guarantees reliability in the delivery of data, and it provides indication of a connection loss.
>
> 2. Network Computing Architecture Datagram Protocol (NCADG)
>
> This connectionless protocol runs over connectionless transport protocols, such as UDP. DG does it "as best as it can". Packets are individually addressed. They can follow different network paths; therefore, the sequence of the incoming packets may be mixed up. Packets can get lost. Reliability must be provided by higher layers; it is not protocol-inherent. DG protocol supports broadcast calls. Lendenmann at 179.

Accordingly, Lendenmann anticipates claim 15 of the '181 patent under 35 U.S.C. § 102(b).

14. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

Lendenmann discloses that the CDS, from which the network address associated with the secure name of a second device is obtained, is integrated into the security services featured in the DCE system. For example:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations. Lendenmann at 34.

A significant part of the authentication concepts of the DCE Security Service described in Lendenmann "are keys and tickets. Keys are used to encrypt/decrypt messages." Lendenmann at 57.

Accordingly, Lendenmann anticipates claim 18 of the '181 patent under 35 U.S.C. § 102(b).

15. Claim 19

Claim 19 depends from claim 2 and specifies "wherein the first device is a computer, and the steps are performed on the computer."

The DCE system disclosed in Lendenmann is "is a layer of services that allows distributed applications to communicate with a collection of computers, operating systems and networks. This collection of machines, operating systems and networks, when managed by a single set of DCE services, is referred to as a DCE cell." Lendenmann at 57.

Accordingly, Lendenmann anticipates claim 19 of the '181 patent under 35 U.S.C. § 102(b).

16. Claim 20

Claim 20 depends from claim 2 and specifies "wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network."

The DCE system disclosed in Lendenmann is "is a layer of services that allows distributed applications to communicate with a collection of computers, operating systems and networks. This collection of machines, operating systems and networks, when managed by a single set of DCE services, is referred to as a DCE cell." Lendenmann at 57.

Accordingly, Lendenmann anticipates claim 20 of the '181 patent under 35 U.S.C. § 102(b).

17. Claim 21

Claim 21 depends from claim 2 and specifies "further including providing an unsecured name associated with the device."

The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. It also enables users to identify and access foreign cells over the internet utilizing an unsecure name. Lendenmann at 23. The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.
>
> There are two well-established naming schemes in place that DCE makes use of:
>
> - CCITT X.500
> - Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. *see also*, "Intercell Routing Services," Lendenmann at 26 ("The GDS client passes the request to a GDS server, which can be anywhere in the whole global network. If the name is a DNS name, the GDA passes the request to its local DNS server to resolve the address of the foreign cell.")

Accordingly, Lendenmann anticipates claim 21 of the '181 patent under 35 U.S.C. § 102(b).

18. Claim 22

Claim 22 depends from claim 2 and specifies "wherein the secure name is registered prior to the step of sending a message to a secure name service."

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry." Lendenmann at 178-79.

In particular, Lendenmann describes that exporting information, i.e. registering information, into an RPC server can be performed by an administrator or the server itself. For example:

> An administrator may be involved in registering servers in the namespace, but this can also be done by the server itself upon initialization. Otherwise, the administrator might have to use the dcecp command (OSF DCE 1.1) or the rpccp command (DCE 1.0.x), which is still available, to manually register this information. An application can provide a configuration tool (or a script written in dcecp) to create static entries in the namespace.
>
> Authorized individuals can add entries to and remove them from the namespace, or they can add information to and remove it from those entries. In the example below, we assume that there are two CDS directories: /.:/home and /.:/servers. Lendenmann at 203.

As indicated above, names in the CDS namespace are secure:

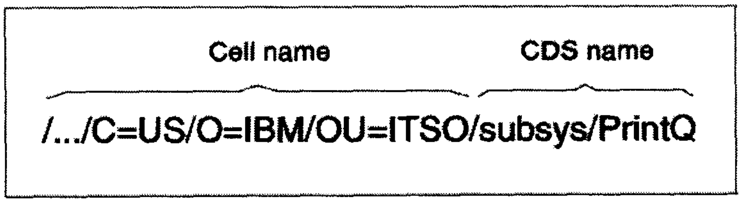
> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations.
>
> CDS authorization allows you to control user access to:
>
> - ***Names in the namespace***, including clearinghouses, directories, object entries, soft links, and child pointers
>
> - Execution of privileged CDS clerk and server commands
>
> Access control is done by creating access control lists (ACL) that contain individual ACL entries that determine which user (principal) ***can use the name*** and what management operations they are allowed to perform on it. Lendenmann at 34.

Accordingly, Lendenmann anticipates claim 22 of the '181 patent under 35 U.S.C. § 102(b).

19. Claim 23

Claim 23 depends from claim 2 and specifies "wherein the secure name of the second device is a secure, non-standard domain name."

The CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500



naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

Lendenmann describes the components of the secure domain name represented by the X.500 naming scheme:

> Figure 9 shows a global name that refers to a printer queue object defined in the IBM ITSO cell. Local users can address it with /.:/susbsys/PrintQ. The prefix (/...) indicates that the name is global. Following the prefix, the X.500 syntax defines four blocks, each one with two parts separated by an equal sign (=). The abbreviation of each block stands for country (C), organization (O), organizational unit (OU), and common name (CN, not shown). Lendenmann at 23.

Moreover, as discussed in section III above, VirnetX responded to an office action rejection during prosecution of the '181 patent by, among other things, stating that a telephone number is one example of a non-standard domain name. Just as a telephone number locates a particular interface or service on a particular multimedia device, e.g., the telephony service of a cell phone, certain names, like 'fax_if,' in OSF DCE locate particular interfaces on particular devices, as well. *See, e.g.*, 'fax_if' shown in Figure 66 below, which locates a fax service on a particular host:

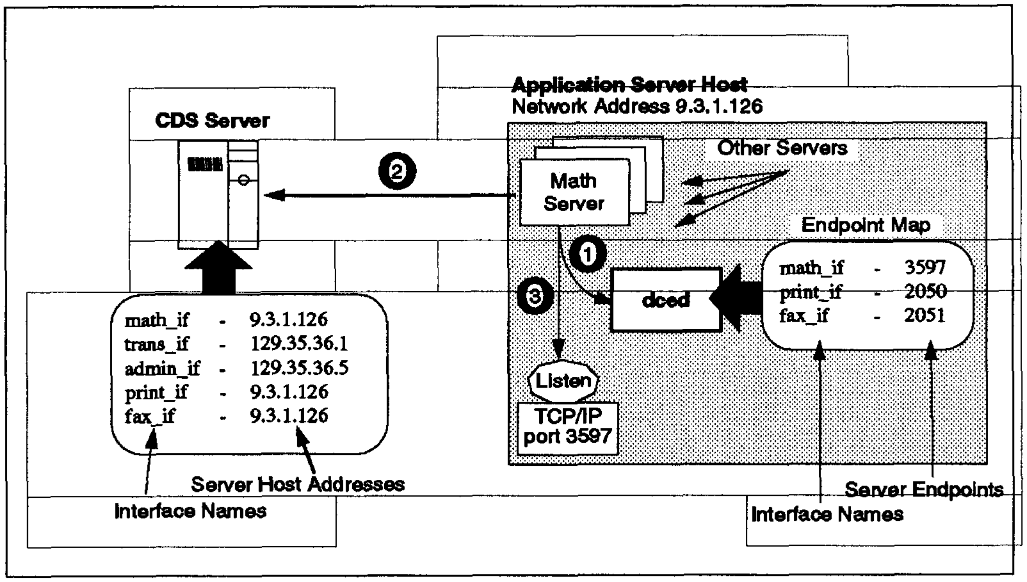


Figure 66. Server Initialization

Lendenmann at 181.

Accordingly, Lendenmann anticipates claim 23 of the '181 patent under 35 U.S.C. § 102(b).

20. Claim 24

Independent claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network, the method comprising:

(a) at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;

(b) receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and

(c) sending a message securely from the first device to the second device."

The preamble of claim 24 specifies "[a] method of using a first device to securely communicate with a second device over a communication network. . . ." The Open Software Foundation Distributed Computing Environment ("DCE") is a software system touting "a set of integrated services designed to support the development and use of distributed applications" in order to facilitate secure communications among devices within the DC. Lendenmann at 1. Each device within a DCE is associated with one or more secure and unsecured names. In a DCE, names can be assigned to each application, server, client, and/or machine. Multiple applications and/or servers can reside on a single machine, and the name of each machine, application, and server is contained in a DNS-type look-up service, called the Cell Directory Server ("CDS"). A query to the CDS using the disclosed application and/or devices results in the return of the IP address of the device and/or application queried. This collection of applications, servers, and/or services is referred to in OSF DCE as "network resources." Each DCE Cell is further represented in the Internet DNS system with an unsecured name.

In the DCE environment, a DCE Cell is a collection of machines that comprise a Security Server and a Cell Directory Server. For example:

> The collection of machines that are managed together as a DCE unit is referred to as a *cell.* At a minimum, a cell must contain a Security Server, a Cell Directory Server and Distributed Time Servers. All of these services may run on one machine, or the servers can be spread among the machines that are to be part of the cell. The Directory, Time and Security Services are collectively known as the core services. Lendenmann at 9.

DCE Directory Services allow users to identify, by name, network resources for access using either a DNS name or a CCITT X.500 name:

> The Directory Service provides a naming model throughout the distributed environment that allows users to identify, by name, network resources, such as servers, users, files, disks, or print queues. The DCE Directory Service includes:

> - Cell Directory Service (CDS)
> - Global Directory Service (GDS)
> - Global Directory Agent (GDA)
> - Application Programming Interface (API)
>
> The CDS manages information within a cell. The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

When a client within a particular DCE cell desires to communicate with the host in different DCE cell—presumably across the Internet—the client may utilize the disclosed DNS system in order to obtain the IP address of the CDS in the different cell. After obtaining the IP address of the "foreign" CDS server, the client queries the foreign CDS server for the IP address of the desired host in the "foreign" network. The local CDS then returns the IP address of the desired host in the foreign cell to the requesting client. The DNS record in the public DNS is thus an unsecured name associated with the foreign cell, i.e., is associated with all hosts in the foreign cell. Lendenmann at 8-10, 23.

The client-server architecture described in Lendenmann is not limited to a traditional client-server understanding. Instead, the disclosed system contemplates that a single device is able to play the role of both client and server. Lendenmann discloses, for example:

> The terms client and server can refer to the role of a single application. For example, machine A may have a program that requests a piece of information from another machine, B. In this example, the program running on machine A is assuming the role of a client, while the program on machine B that fulfills the request is acting as the server. It is not hard to imagine that in a multitasking operating system environment we may have both client and server applications running on the same machine at the same time. It is also not hard to see that both the client and server functions for a transaction may both run on the same machine. In many cases, it will be necessary for the machine running the server to also run the client application in order to obtain access to the function it is serving. Lendenmann at 8-9.

The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. It also enables users to identify and access foreign cells over the internet utilizing an unsecure name. Lendenmann at 23. The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.
>
> There are two well-established naming schemes in place that DCE makes use of:
>
> - CCITT X.500
> - Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

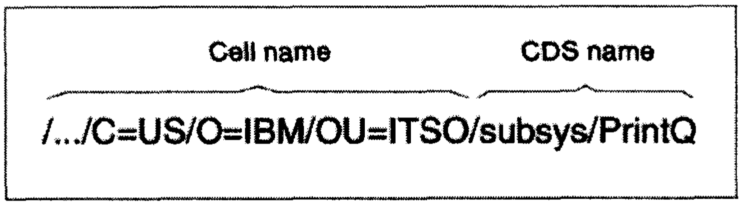


Figure 9. Global Representation of a Subsystem Printer Queue

Further, the distinction between the X.500 and DNS naming conventions can be distilled, for example, from the Figure 10 in Lendenmann:

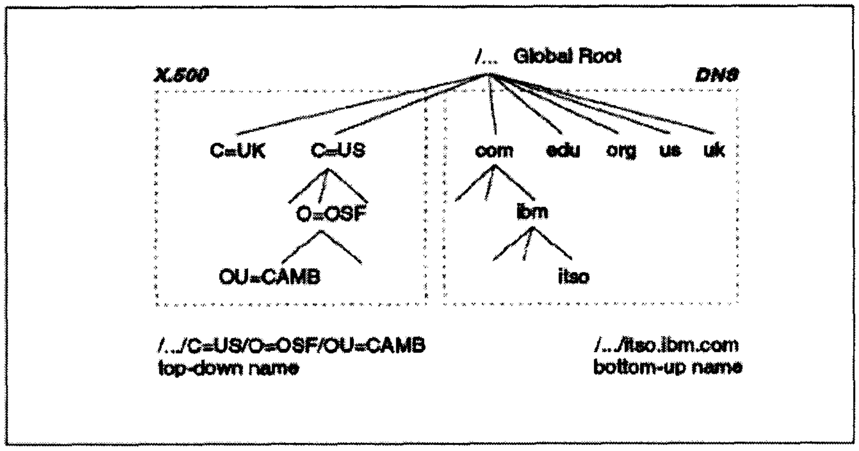


Figure 10. Comparison of Cell Name Representations

Lendenmann shows that a given device in the DCE system is able to have multiple names through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Thus, Lendenmann discloses "method of using a first device to securely communicate with a second device over a communication network."

Step (a) of Claim 24 specifies "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address"

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry." Lendenmann at 178-79.

In particular, Lendenmann describes that exporting information, i.e. registering information, into an RPC server can be performed by an administrator or the server itself. For example:

> An administrator may be involved in registering servers in the namespace, but this can also be done by the server itself upon initialization. Otherwise, the administrator might have to use the dcecp command (OSF DCE 1.1) or the rpccp command (DCE 1.0.x), which is still available, to manually register this information. An application can provide a configuration tool (or a script written in dcecp) to create static entries in the namespace.

> Authorized individuals can add entries to and remove them from the namespace, or they can add information to and remove it from those entries. In the example below, we assume that there are two CDS directories: /.:/home and /.:/servers. Lendenmann at 203.

Lendenmann teaches the names in the CDS namespace are secure names:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations.
>
> CDS authorization allows you to control user access to:
>
> - ***Names in the namespace***, including clearinghouses, directories, object entries, soft links, and child pointers
> - Execution of privileged CDS clerk and server commands
>
> Access control is done by creating access control lists (ACL) that contain individual ACL entries that determine which user (principal) ***can use the name*** and what management operations they are allowed to perform on it.

CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests. When a principal requests an operation on a CDS name or a privileged operation on a CDS clerk or server, ACL management software examines the ACL entry associated with that name or principal name and grants or denies the operation. Lendenmann at 34 (emphasis added).

Thus, Lendenmann discloses "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

Step (b) of claim 24 specifies: "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device"

Lendenmann discloses that devices in DCE—and the distributed client/server applications within—"use remote procedure calls (RPCs) to make function calls (transparently) across a network." Lendenmann at 173. Establishing a relationship in the DCE client/server model requires a "binding" between the client and server. "A binding is a temporary relationship that depends on a communications link." Lendenmann at 174. RPC Runtime, which is a component involved in the processing of an RPC, is responsible for "perform[ing] such tasks as controlling communication between clients and servers or finding servers for the clients on request."

RPC Runtime provides a number of different services. For example, RPC Runtime "is responsible for establishing a binding (the communication link) and for the data transfer between client and server." Lendenmann at 178. RPC is also responsible for providing "Directory service interface operations." Lendenmann at 178. The Directory Service described in

Lendenmann enables users to find other networked objects without knowing their physical location. Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information." Lendenmann at 178-79.

One of the many ways a second device can locate a network address of a first device is through the CDS:

> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a *binding*.... A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the *Name Service Interface* import operations. Lendenmann at 182.

The steps involved in locating the address of another device in represented graphically in Lendenmann in Figure 68:

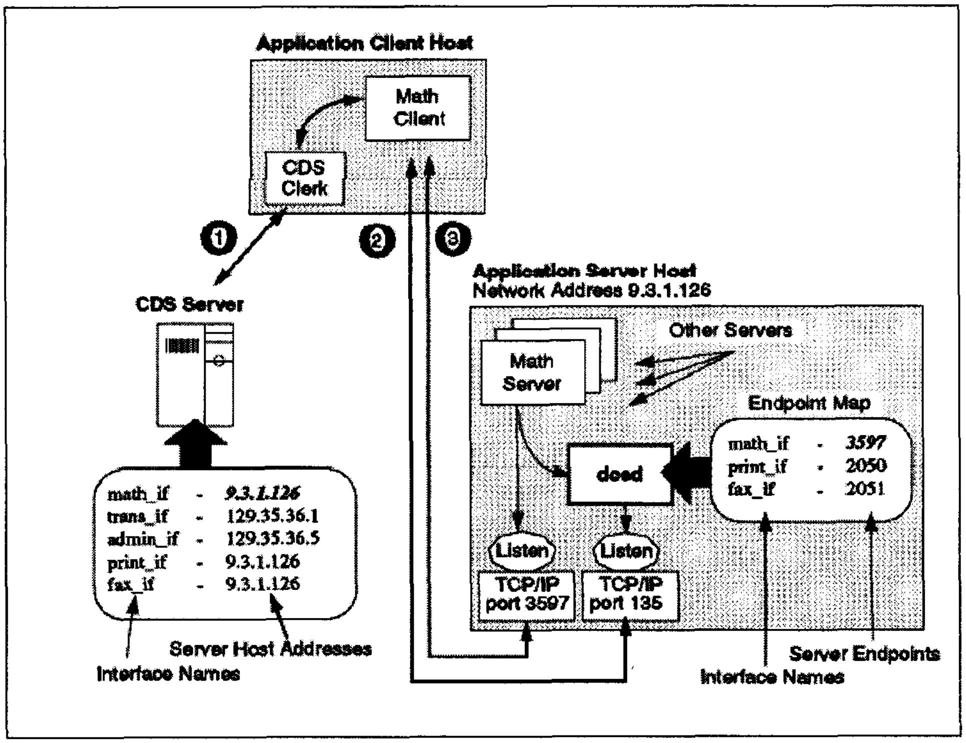


Figure 68. Steps Involved in Finding a Server

The first step in the process, as shown in Figure 68, is looking up the network address information of the server/device that the client/device is seeking to communicate. Once the network is address is known, the client/device's "RPC runtime then directly calls the server process listening to the endpoint." Lendenmann at 191.

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Thus, Lendenmann discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Step (c) of claim 24 specifies: "sending a message securely from the first device to the second device."

As discussed above in **Step (b),** Lendenmann permits users of the system to define the level of security a client/device wants to establish when communicating with another device. Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

- None. No communication protection.
- Connection. Performs an encrypted handshake the first time the client communicates with the server.
- Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
- Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
- Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
- CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.

- Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Thus, Lendenmann discloses "sending a message securely from the first device to the second device."

Accordingly, Lendenmann anticipates claim 24 of the '181 patent under 35 U.S.C. § 102(b).

21. Claim 25

Claim 25 depends from claim 24 and specifies "wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link."

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry." Lendenmann at 178-79.

In particular, Lendenmann describes that exporting information, i.e. registering information, into an RPC server can be performed by an administrator or the server itself. For example:

> An administrator may be involved in registering servers in the namespace, but this can also be done by the server itself upon initialization. Otherwise, the administrator might have to use the dcecp command (OSF DCE 1.1) or the rpccp command (DCE 1.0.x), which is still available, to manually register this information. An application can provide a configuration tool (or a script written in dcecp) to create static entries in the namespace.
>
> Authorized individuals can add entries to and remove them from the namespace, or they can add information to and remove it from those entries. In the example below, we assume that there are two CDS directories: /.:/home and /.:/servers. Lendenmann at 203.

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

> - None. No communication protection.
> - Connection. Performs an encrypted handshake the first time the client communicates with the server.
> - Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
> - Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
> - Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
> - CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.
> - Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Accordingly, Lendenmann anticipates claim 25 of the '181 patent under 35 U.S.C. § 102(b).

22. Claim 26

Independent claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising:

(a) from the first device requesting and obtaining registration of an unsecured name associated with the first device;

(b) from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;

(c) receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

(d) from the first device sending a message securely from the first device to the second device."

The preamble of independent claim 26 specifies "[a] method of using a first device to communication with a second device over a communication network." The Open Software Foundation Distributed Computing Environment ("DCE") is a software system touting "a set of integrated services designed to support the development and use of distributed applications" in order to facilitate secure communications among devices within the DC. Lendenmann at 1. Each device within a DCE is associated with one or more secure and unsecured names. In a DCE, names can be assigned to each application, server, client, and/or machine. Multiple applications and/or servers can reside on a single machine, and the name of each machine, application, and server is contained in a DNS-type look-up service, called the Cell Directory Server ("CDS"). A query to the CDS using the disclosed application and/or devices results in the return of the IP address of the device and/or application queried. This collection of applications, servers, and/or services is referred to in OSF DCE as "network resources." Each DCE Cell is further represented in the Internet DNS system with an unsecured name.

In the DCE environment, a DCE Cell is a collection of machines that comprise a Security Server and a Cell Directory Server. For example:

> The collection of machines that are managed together as a DCE unit is referred to as a *cell.* At a minimum, a cell must contain a Security Server, a Cell Directory Server and Distributed Time Servers. All of these services may run on one machine, or the servers can be spread among the machines that are to be part of the cell. The Directory, Time and Security Services are collectively known as the core services. Lendenmann at 9.

DCE Directory Services allow users to identify, by name, network resources for access using either a DNS name or a CCITT X.500 name:

> The Directory Service provides a naming model throughout the distributed environment that allows users to identify, by name, network resources, such as servers, users, files, disks, or print queues. The DCE Directory Service includes:
>
> - Cell Directory Service (CDS)
> - Global Directory Service (GDS)
> - Global Directory Agent (GDA)
> - Application Programming Interface (API)
>
> The CDS manages information within a cell. The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both

> Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

When a client within a particular DCE cell desires to communicate with the host in different DCE cell—presumably across the Internet—the client may utilize the disclosed DNS system in order to obtain the IP address of the CDS in the different cell. After obtaining the IP address of the "foreign" CDS server, the client queries the foreign CDS server for the IP address of the desired host in the "foreign" network. The local CDS then returns the IP address of the desired host in the foreign cell to the requesting client. The DNS record in the public DNS is thus an unsecured name associated with the foreign cell, i.e., is associated with all hosts in the foreign cell. Lendenmann at 8-10, 23.

The client-server architecture described in Lendenmann is not limited to a traditional client-server understanding. Instead, the disclosed system contemplates that a single device is able to play the role of both client and server. Lendenmann discloses, for example:

> The terms client and server can refer to the role of a single application. For example, machine A may have a program that requests a piece of information from another machine, B. In this example, the program running on machine A is assuming the role of a client, while the program on machine B that fulfills the request is acting as the server. It is not hard to imagine that in a multitasking operating system environment we may have both client and server applications running on the same machine at the same time. It is also not hard to see that both the client and server functions for a transaction may both run on the same machine. In many cases, it will be necessary for the machine running the server to also run the client application in order to obtain access to the function it is serving. Lendenmann at 8-9.

The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. It also enables users to identify and access foreign cells over the internet utilizing an unsecure name. Lendenmann at 23. The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.

There are two well-established naming schemes in place that DCE makes use of:

- CCITT X.500
- Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

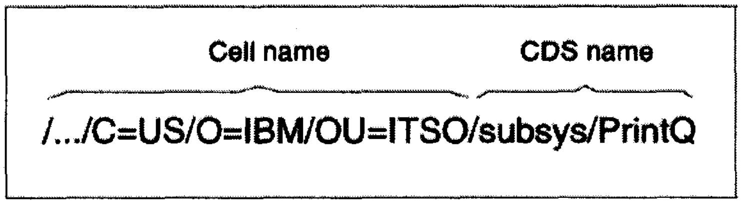


Figure 9. Global Representation of a Subsystem Printer Queue

Further, the distinction between the X.500 and DNS naming conventions can be distilled, for example, from the Figure 10 in Lendenmann:

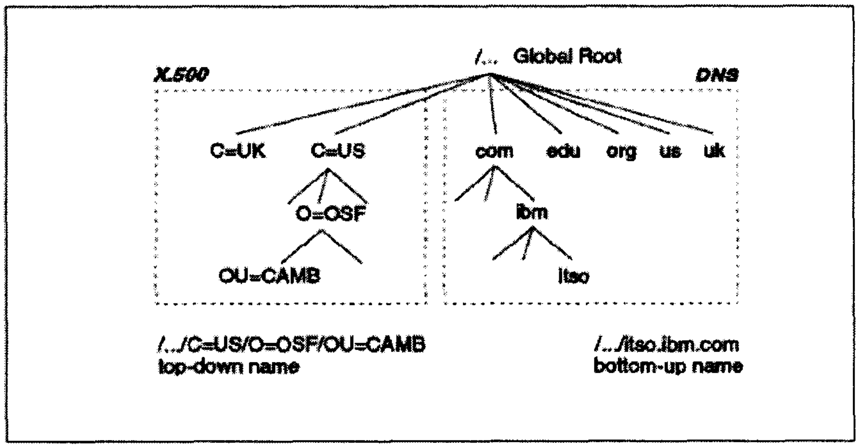


Figure 10. Comparison of Cell Name Representations

Thus, the use of the DCE system permits devices anywhere in the DCE system to obtain the network address of any other device in order to engage in communications.

Thus, Lendenmann discloses "[a] method of using a first device to communicate with a second device over a communication network."

Step (a) of claim 26 specifies: "from the first device requesting and obtaining registration of an unsecured name associated with the first device"

Lendenmann shows that a given device in the DCE system is able to have multiple names—secure and unsecured—through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name." The DCE system includes the capability fore registering a DNS name in addition to the GDS name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Thus, Lendenmann discloses: "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Step (b) of claim 26 specifies: "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device"

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry." Lendenmann at 178-79.

In particular, Lendenmann describes that exporting information, i.e. registering information, into an RPC server can be performed by an administrator or the server itself. For example:

> An administrator may be involved in registering servers in the namespace, but this can also be done by the server itself upon initialization. Otherwise, the administrator might have to use the dcecp command (OSF DCE 1.1) or the rpccp command (DCE 1.0.x), which is still available, to manually register this information. An application can provide a configuration tool (or a script written in dcecp) to create static entries in the namespace.
>
> Authorized individuals can add entries to and remove them from the namespace, or they can add information to and remove it from those entries. In the example below, we assume that there are two CDS directories: /.:/home and /.:/servers. Lendenmann at 203.

Thus, Lendenmann discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Step (c) of claim 26 specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device"

Lendenmann discloses that devices in DCE—and the distributed client/server applications within—"use remote procedure calls (RPCs) to make function calls (transparently) across a network." Lendenmann at 173. Establishing a relationship in the DCE client/server model requires a "binding" between the client and server. "A binding is a temporary relationship that depends on a communications link." Lendenmann at 174. RPC Runtime, which is a component involved in the processing of an RPC, is responsible for "perform[ing] such tasks as controlling communication between clients and servers or finding servers for the clients on request."

RPC Runtime provides a number of different services. For example, RPC Runtime "is responsible for establishing a binding (the communication link) and for the data transfer between client and server." Lendenmann at 178. RPC is also responsible for providing "Directory service interface operations." Lendenmann at 178. The Directory Service described in Lendenmann enables users to find other networked objects without knowing their physical location. Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information." Lendenmann at 178-79.

One of the many ways a second device can locate a network address of a first device is through the CDS:

> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a *binding*.... A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the *Name Service Interface* import operations. Lendenmann at 182.

The steps involved in locating the address of another device in represented graphically in Lendenmann in Figure 68:

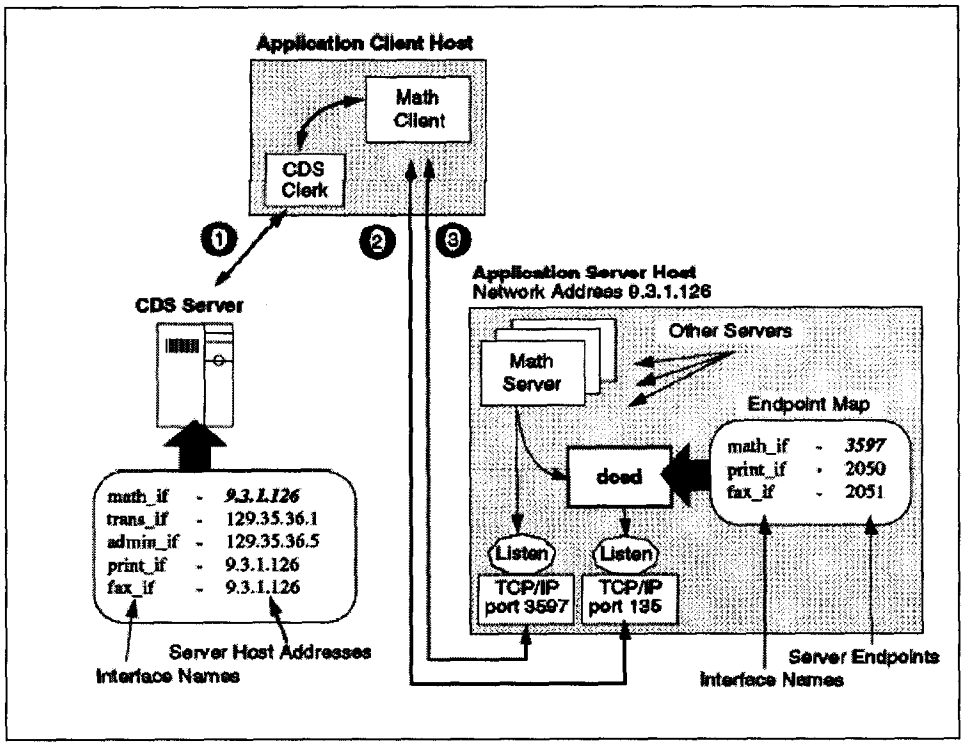


Figure 68. Steps Involved in Finding a Server

The first step in the process, as shown in Figure 68, is looking up the network address information of the server/device that the client/device is seeking to communicate. Once the network is address is known, the client/device's "RPC runtime then directly calls the server process listening to the endpoint." Lendenmann at 191.

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Thus, Lendenmann discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Thus, Lendenmann discloses "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device."

Step (d) of claim 26 specifies: "from the first device sending a message securely from the first device to the second device."

As discussed above in **Step (c),** Lendenmann permits users of the system to define the level of security a client/device wants to establish when communicating with another device. Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

- None. No communication protection.
- Connection. Performs an encrypted handshake the first time the client communicates with the server.
- Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
- Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
- Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
- CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF. Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Thus, Lendenmann discloses "from the first device sending a message securely from the first device to the second device."

Accordingly, Lendenmann anticipates claim 26 of the '181 patent under 35 U.S.C. § 102(b).

23. Claim 27

Claim 27 depends from claim 26 and specifies:

(a) "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

> (b) wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Step (a) of claim 27 specifies: "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

Lendenmann shows that a given device in the DCE system is able to have multiple names—secure and unsecured—through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name." The DCE system includes the capability for registering a DNS name in addition to the GDS name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Lendenmann describes commands that a user may initiate from a device in order to register a cell name in DNS. Lendenmann at 24.

Thus, Lendenmann discloses: "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device."

Step (b) of claim 27 specifies: wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry." Lendenmann at 178-79.

In particular, Lendenmann describes that exporting information, i.e. registering information, into an RPC server can be performed by an administrator or the server itself. For example:

> An administrator may be involved in registering servers in the namespace, but this can also be done by the server itself upon initialization. Otherwise, the administrator might have to use the dcecp command (OSF DCE 1.1) or the rpccp command (DCE 1.0.x), which is still available, to manually register this information. An application can provide a configuration tool (or a script written in dcecp) to create static entries in the namespace.

> Authorized individuals can add entries to and remove them from the namespace, or they can add information to and remove it from those entries. Lendenmann at 203.

Accordingly, Lendenmann anticipates claim 27 of the '181 patent under 35 U.S.C. § 102(b).

24. Claim 28

Independent claim 28 is directed to "[a] non-transitory machine-readable medium comprising instructions for:

(a) sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

(b) receiving a message containing the network address associated with the secure name of the device; and

(c) sending a message to the network address associated with the secure name of the device using a secure communication link.

The preamble of claim 28 specifies "[a] -transitory machine-readable medium comprising instructions. . . ." The Open Software Foundation Distributed Computing Environment ("DCE") is a software system touting "a set of integrated services designed to support the development and use of distributed applications" in order to facilitate secure communications among devices within the DC. Lendenmann at 1.

Thus, Lendenmann discloses "[a] transitory machine-readable medium comprising instructions."

Step (a) of Claim 28 specifies: "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

Each device within a DCE is associated with one or more secure and unsecured names. In a DCE, names can be assigned to each application, server, client, and/or machine. Multiple applications and/or servers can reside on a single machine, and the name of each machine, application, and server is contained in a DNS-type look-up service, called the Cell Directory Server ("CDS"). A query to the CDS using the disclosed application and/or devices results in the return of the IP address of the device and/or application queried. This collection of applications, servers, and/or services is referred to in OSF DCE as "network resources." Each DCE Cell is further represented in the Internet DNS system with an unsecured name.

Lendenmann teaches the CDS is a secure name service:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and

> authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations.
>
> CDS authorization allows you to control user access to:
>
> - ***Names in the namespace***, including clearinghouses, directories, object entries, soft links, and child pointers
> - Execution of privileged CDS clerk and server commands
>
> Access control is done by creating access control lists (ACL) that contain individual ACL entries that determine which user (principal) ***can use the name*** and what management operations they are allowed to perform on it.

CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests. When a principal requests an operation on a CDS name or a privileged operation on a CDS clerk or server, ACL management software examines the ACL entry associated with that name or principal name and grants or denies the operation. Lendenmann at 34 (emphasis added).

In the DCE environment, a DCE Cell is a collection of machines that comprise a Security Server and a Cell Directory Server. For example:

> The collection of machines that are managed together as a DCE unit is referred to as a *cell.* At a minimum, a cell must contain a Security Server, a Cell Directory Server and Distributed Time Servers. All of these services may run on one machine, or the servers can be spread among the machines that are to be part of the cell. The Directory, Time and Security Services are collectively known as the core services. Lendenmann at 9.

DCE Directory Services allow users to identify, by name, network resources for access using either a DNS name or a CCITT X.500 name:

> The Directory Service provides a naming model throughout the distributed environment that allows users to identify, by name, network resources, such as servers, users, files, disks, or print queues. The DCE Directory Service includes:
>
> - Cell Directory Service (CDS)
> - Global Directory Service (GDS)
> - Global Directory Agent (GDA)
> - Application Programming Interface (API)
>
> The CDS manages information within a cell. The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service

> (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

When a client within a particular DCE cell desires to communicate with the host in different DCE cell—presumably across the Internet—the client may utilize the disclosed DNS system in order to obtain the IP address of the CDS in the different cell. After obtaining the IP address of the "foreign" CDS server, the client queries the foreign CDS server for the IP address of the desired host in the "foreign" network. The local CDS then returns the IP address of the desired host in the foreign cell to the requesting client. The DNS record in the public DNS is thus an unsecured name associated with the foreign cell, i.e., is associated with all hosts in the foreign cell. Lendenmann at 8-10, 23.

The client-server architecture described in Lendenmann is not limited to a traditional client-server understanding. Instead, the disclosed system contemplates that a single device is able to play the role of both client and server. Lendenmann discloses, for example:

> The terms client and server can refer to the role of a single application. For example, machine A may have a program that requests a piece of information from another machine, B. In this example, the program running on machine A is assuming the role of a client, while the program on machine B that fulfills the request is acting as the server. It is not hard to imagine that in a multitasking operating system environment we may have both client and server applications running on the same machine at the same time. It is also not hard to see that both the client and server functions for a transaction may both run on the same machine. In many cases, it will be necessary for the machine running the server to also run the client application in order to obtain access to the function it is serving. Lendenmann at 8-9.

The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. It also enables users to identify and access foreign cells over the internet utilizing an unsecure name. Lendenmann at 23. The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.
>
> There are two well-established naming schemes in place that DCE makes use of:

- CCITT X.500
- Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

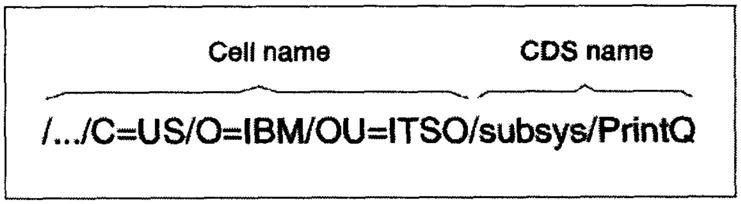


Figure 9. Global Representation of a Subsystem Printer Queue

Further, the distinction between the X.500 and DNS naming conventions can be distilled, for example, from the Figure 10 in Lendenmann:

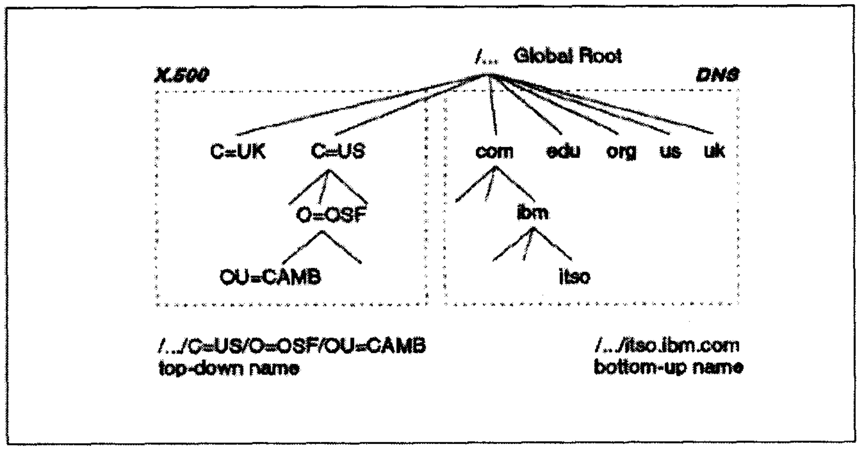


Figure 10. Comparison of Cell Name Representations

Lendenmann shows that a given device in the DCE system is able to have multiple names through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Lendenmann discloses that devices in DCE—and the distributed client/server applications within—"use remote procedure calls (RPCs) to make function calls (transparently) across a network." Lendenmann at 173. Establishing a relationship in the DCE client/server model requires a "binding" between the client and server. "A binding is a temporary relationship that depends on a communications link." Lendenmann at 174. RPC Runtime, which is a component involved in the processing of an RPC, is responsible for "perform[ing] such tasks as controlling communication between clients and servers or finding servers for the clients on request."

RPC Runtime provides a number of different services. For example, RPC Runtime "is responsible for establishing a binding (the communication link) and for the data transfer between client and server." Lendenmann at 178. RPC is also responsible for providing "Directory service interface operations." Lendenmann at 178. The Directory Service described in Lendenmann enables users to find other networked objects without knowing their physical location. Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information." Lendenmann at 178-79.

One of the many ways a second device can locate a network address of a first device is through the CDS:

> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a *binding*.... A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the *Name Service Interface* import operations. Lendenmann at 182.

Thus, Lendenmann shows the step of "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

Step (b) of claim 28 specifies: "receiving a message containing the network address associated with the secure name of the device"

Lendenmann discloses the steps involved in retrieving the address of another device graphically in Figure 68:

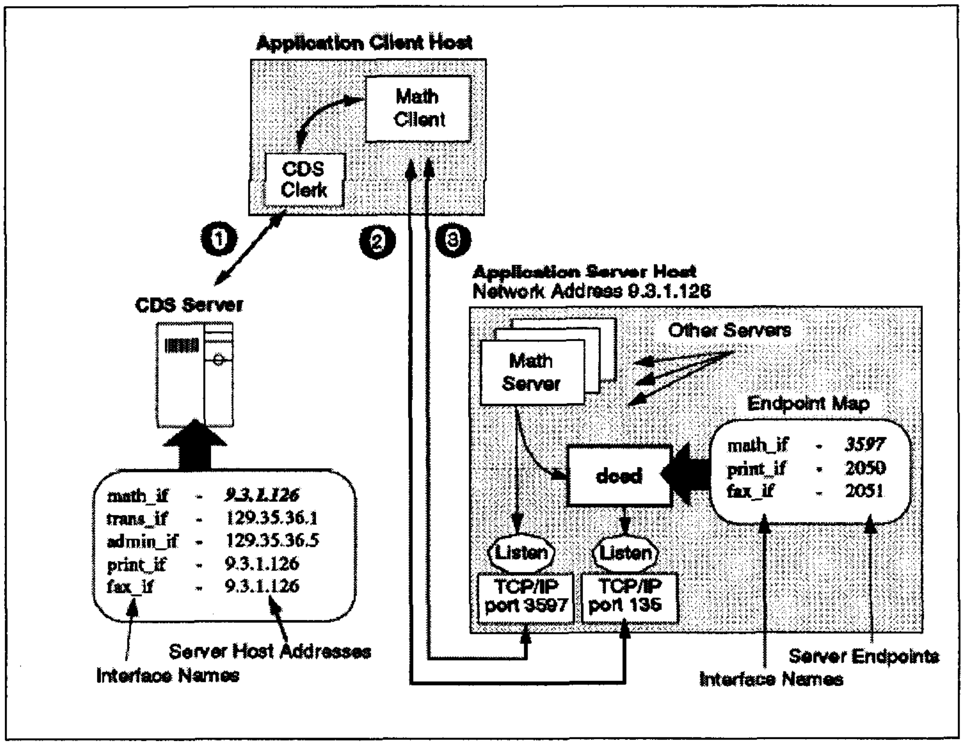


Figure 68. Steps Involved in Finding a Server

The first step in the process, as shown in Figure 68, is looking up the network address information of the server/device that the client/device is seeking to communicate. Once the network is address is known, the client/device's RPC runtime—using the network address information provided by the CDS—"then directly calls the server process listening to the endpoint." Lendenmann at 191.

Thus, Lendenmann shows the step of "receiving a message containing the network address associated with the secure name of the device."

Step (c) of claim 28 specifies: "sending a message to the network address associated with the secure name of the device using a secure communication link."

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

> - None. No communication protection.
> - Connection. Performs an encrypted handshake the first time the client communicates with the server.
> - Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
> - Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.
> - Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
> - CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.
> - Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Thus, Lendenmann shows the step of "sending a message to the network address associated with the secure name of the device using a secure communication link."

Accordingly, Lendenmann anticipates claim 28 of the '181 patent under 35 U.S.C. § 102(b).

25. Claim 29

Independent claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

> (a) receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and
>
> (b) sending a message securely from the first device to the second device.

The preamble of claim 29 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name . . .

." The Open Software Foundation Distributed Computing Environment ("DCE") is a software system touting "a set of integrated services designed to support the development and use of distributed applications" in order to facilitate secure communications among devices within the DC. Lendenmann at 1. Each device within a DCE is associated with one or more secure and unsecured names. In a DCE, names can be assigned to each application, server, client, and/or machine. Multiple applications and/or servers can reside on a single machine, and the name of each machine, application, and server is contained in a DNS-type look-up service, called the Cell Directory Server ("CDS"). A query to the CDS using the disclosed application and/or devices results in the return of the IP address of the device and/or application queried. This collection of applications, servers, and/or services is referred to in OSF DCE as "network resources." Each DCE Cell is further represented in the Internet DNS system with an unsecured name.

Lendenmann teaches the CDS is a secure name service:

> 2.5 Security in CDS Environment
>
> The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized by the Security Service. It is a two-way process where the user or the principal is first authenticated to prove who he is and then authorized to do certain operations.
>
> CDS authorization allows you to control user access to:
>
> - ***Names in the namespace***, including clearinghouses, directories, object entries, soft links, and child pointers
> - Execution of privileged CDS clerk and server commands
>
> Access control is done by creating access control lists (ACL) that contain individual ACL entries that determine which user (principal) ***can use the name*** and what management operations they are allowed to perform on it.

CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests. When a principal requests an operation on a CDS name or a privileged operation on a CDS clerk or server, ACL management software examines the ACL entry associated with that name or principal name and grants or denies the operation. Lendenmann at 34 (emphasis added).

In the DCE environment, a DCE Cell is a collection of machines that comprise a Security Server and a Cell Directory Server. For example:

> The collection of machines that are managed together as a DCE unit is referred to as a *cell*. At a minimum, a cell must contain a Security Server, a Cell Directory Server and Distributed Time Servers. All of these services may run on one machine, or the servers can be spread among the machines that are to be part of the cell. The Directory, Time and Security Services are collectively known as the core services. Lendenmann at 9.

DCE Directory Services allow users to identify, by name, network resources for access using either a DNS name or a CCITT X.500 name:

> The Directory Service provides a naming model throughout the distributed environment that allows users to identify, by name, network resources, such as servers, users, files, disks, or print queues. The DCE Directory Service includes:
>
> - Cell Directory Service (CDS)
> - Global Directory Service (GDS)
> - Global Directory Agent (GDA)
> - Application Programming Interface (API)
>
> The CDS manages information within a cell. The GDS is based on the CCITT X.500 name schema and provides the basis for a global namespace. The GDA is the CDS gateway to intercell communication. The GDA supports both Internet addresses and X.500 addresses. If the address passed to the GDA is an X.500 address, the GDA contacts the GDS. If the address passed to GDA is an Internet address, then the GDA uses the Internet Domain Name Service (DNS) to locate the foreign cell. Both CDS and GDS use the X/Open Directory Service (XDS) API as a programming interface. Lendenmann at 10.

When a client within a particular DCE cell desires to communicate with the host in different DCE cell—presumably across the Internet—the client may utilize the disclosed DNS system in order to obtain the IP address of the CDS in the different cell. After obtaining the IP address of the "foreign" CDS server, the client queries the foreign CDS server for the IP address of the desired host in the "foreign" network. The local CDS then returns the IP address of the desired host in the foreign cell to the requesting client. The DNS record in the public DNS is thus an unsecured name associated with the foreign cell, i.e., is associated with all hosts in the foreign cell. Lendenmann at 8-10, 23.

The client-server architecture described in Lendenmann is not limited to a traditional client-server understanding. Instead, the disclosed system contemplates that a single device is able to play the role of both client and server. Lendenmann discloses, for example:

> The terms client and server can refer to the role of a single application. For example, machine A may have a program that requests a piece of information from another machine, B. In this example, the program running on machine A is assuming the role of a client, while the program on machine B that fulfills the request is acting as the server. It is not hard to imagine that in a multitasking operating system environment we may have both client and server applications running on the same machine at the same time. It is also not hard to see that both the client and server functions for a transaction may both run on the same machine. In many cases, it will be necessary for the machine running the server to also run the client application in order to obtain access to the function it is serving. Lendenmann at 8-9.

The DCE Global Naming Environment described by Lendenmann provides the model for naming schemes throughout a distributed network. Lendenmann at 22. In particular, the DCE

Naming Service enables users to identify resources within the DCE by a secure name that permits access to those resources without knowing the associated network address. Lendenmann at 23. It also enables users to identify and access foreign cells over the internet utilizing an unsecure name. Lendenmann at 23. The naming schemes described in Lendenmann thus comprise both secure and unsecure names. For example, Lendenmann teaches use of the CCITT X.500 and the Internet Domain Name Service (DNS):

> To be globally addressable, cell names must be unique. There must be an administration authority that keeps track of names and assigns new, unique names. Furthermore, there must be some global network routing mechanism that can find a communication path to the requested cell so that a foreign cell can be accessed.
>
> There are two well-established naming schemes in place that DCE makes use of:
>
> - CCITT X.500
> - Internet Domain Name Service (DNS). Lendenmann at 23.

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Lendenmann at 23. Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." Lendenmann at 23. An example of an X.500 name is shown below:

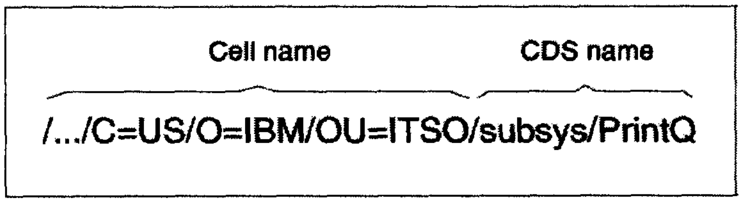


Figure 9. Global Representation of a Subsystem Printer Queue

Further, the distinction between the X.500 and DNS naming conventions can be distilled, for example, from the Figure 10 in Lendenmann:

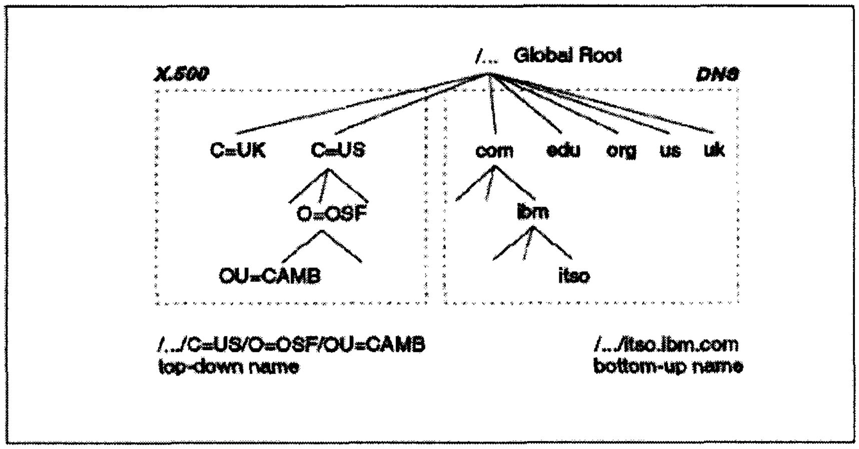


Figure 10. Comparison of Cell Name Representations

Lendenmann shows that a given device in the DCE system is able to have multiple names through a function termed "cell-name aliasing." Cell-name aliasing permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name. For example:

> [I]f your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias. The GDS name remains the primary name. Lendenmann at 24.

Thus, Lendenmann discloses "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name."

Step (a) of Claim 29 specifies: "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered"

Lendenmann discloses that devices in DCE—and the distributed client/server applications within—"use remote procedure calls (RPCs) to make function calls (transparently) across a network." Lendenmann at 173. Establishing a relationship in the DCE client/server model requires a "binding" between the client and server. "A binding is a temporary relationship that depends on a communications link." Lendenmann at 174. RPC Runtime, which is a component involved in the processing of an RPC, is responsible for "perform[ing] such tasks as controlling communication between clients and servers or finding servers for the clients on request."

RPC Runtime provides a number of different services. For example, RPC Runtime "is responsible for establishing a binding (the communication link) and for the data transfer between client and server." Lendenmann at 178. RPC is also responsible for providing "Directory service interface operations. Lendenmann at 178. The Directory Service described in Lendenmann enables users to find other networked objects without knowing their physical location.

Lendenmann describes the Directory Service as "like a telephone directory assistance service that provides the phone number when given a person's name." The Directory Service component that controls the names and addresses of those objects within a DCE cell is called the Cell Directory Service. The CDS can be accessed through the RPC Runtime "RPC Name Service Interface (NSI). Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information." Lendenmann at 178-79.

One of the many ways a second device can locate a network address of a first device is through the CDS:

> The process of finding the server and establishing a relationship over a communication link between the client and server RPC runtimes is called a *binding*.... A client can find a server by asking the CDS for the location of a server that handles the interface that the client is interested in. This is done using the *Name Service Interface* import operations. Lendenmann at 182.

The steps involved in locating the address of another device in represented graphically in Lendenmann in Figure 68:

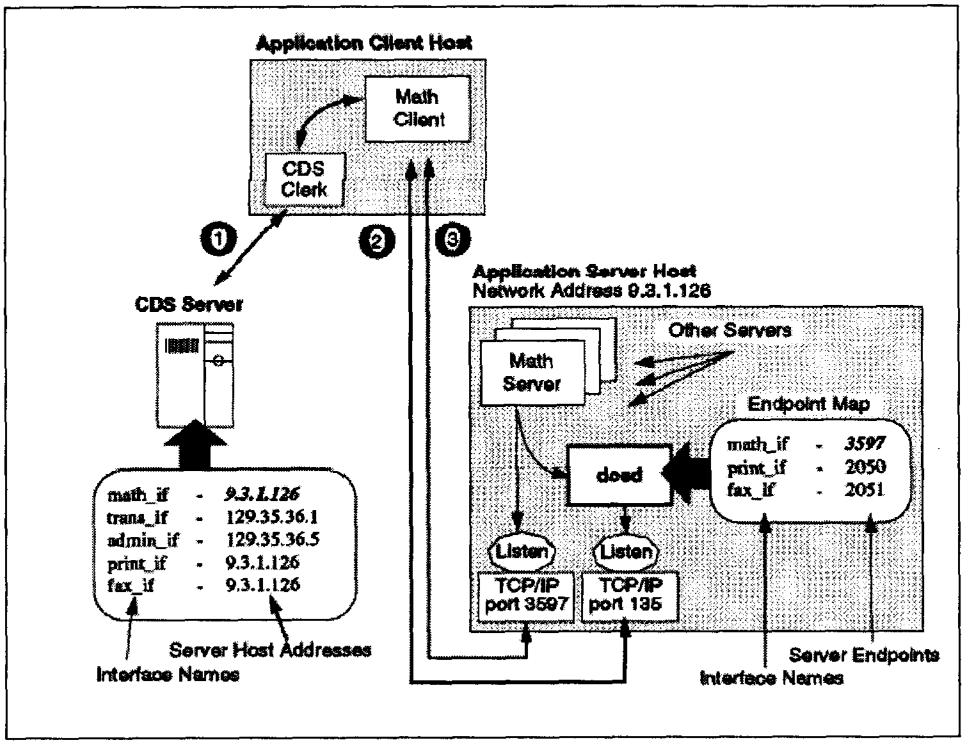


Figure 68. Steps Involved in Finding a Server

The first step in the process, as shown in Figure 68, is looking up the network address information of the server/device that the client/device is seeking to communicate. Once the network is address is known, the client/device's "RPC runtime then directly calls the server process listening to the endpoint." Lendenmann at 191.

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Thus, Lendenmann discloses "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered."

Step (b) of claim 29 specifies: "sending a message securely from the first device to the second device."

Lendenmann also permits users of the system to define the level of security it wants to establish when communicating with another device:

> When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted. Lendenmann at 192.

Lendenmann further explains that DCE can implement a number of security measures for engaging in secure communication. For example:

> 3.5 Security with RPC
>
> Authentication, authorization and data protection are provided with the RPC runtime facility to enable applications to use the DCE Security Service for their RPC communication. Basically, RPC application servers define, during their initialization, what authentication, authorization and data protection levels they support. RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server. Lendenmann at 71.

Lendenmann details some of the different protection levels that are available:

- None. No communication protection.
- Connection. Performs an encrypted handshake the first time the client communicates with the server.
- Call. Attaches an encrypted verifier only at the beginning of each remote procedure call over connectionless communication. This level does not apply for TCP connections.
- Packet. Attaches a verifier to each message sent over the network to make sure all messages are from the expected client.

- Packet Integrity. Ensures and verifies that no messages have been modified by computing and encrypting a checksum over each message.
- CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF.
- Packet Privacy. Encrypts RPC arguments and data in each call using DES. Lendenmann at 192.

Thus, Lendenmann shows the step of "sending a message securely from the first device to the second device."

Accordingly, Lendenmann anticipates claim 29 of the '181 patent under 35 U.S.C. § 102(b).

B. Ground Nos. 7-8: Claims 10-11 and 16-17 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Lendenmann in view of Beser and RFC 2401.

1. Relevant Teachings of the Primary Reference

A detailed explanation of how Lendenmann anticipates claim 2 is provided in **§§ IV.A.1, 2.**

2. Relevant Teachings of the Secondary References

a. Relevant Teachings of Beser

Beser generally describes methods and systems for establishing a secure communication link via a tunneling association in a data network. Beser explains that its method involves "negotiating private addresses, such as private Internet Address, for the ends of the tunneling association." *See* Beser, Abstract. Beser further explains that:

> The negotiation is performed on a public network, such as the Internet, through a trusted-third party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network. Beser, Abstract.

Beser explains that its methods involve a first and second network device, and a "trusted-third-party network device." According to Beser, the first and second network device "may be modified routers or modified gateways." Beser at 4:7-11. Beser further explains that in an exemplary preferred embodiment, the first or second network devices is an "edge router," which Beser explains "routes data packets between one or more networks such as a backbone network (e.g., a public network 12) and Local Area Networks (e.g., private network 20)." *Id.* at 4:19-24. An edge router is a computer, as it has a CPU, memory and storage.

Beser further explains that "the data network also includes network devices (24, 26) that are originating and terminating ends of data flow." *Id.* at 4:43-44. Beser indicates that these devices can include telephony and multimedia devices, and that data that is to be transmitted through the IP tunnels made by the Beser methods can include such telephony or multimedia applications. Beser at 4:.47-50.

b. Relevant Teachings of RFC 2401

Generally, RFC 2401 is concerned with providing high quality security for Internet transactions that is adaptable to particular implementation needs and that facilitates interoperability over the Internet. *See, e.g.,* RFC 2401 at 4-5 ("The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations"; *see also Id.* at 5 ("A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.").

In particular, RFC 2401 defines the IPSec Protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes particular "cases" to implement secure communications involving a VPN, including "Case 3" which describes VPN implementation where edge routers on two different networks are used to establish an encrypted IP tunnel through which the network devices will communicate. RFC 2401 at 24-26.

3. Ground No. 7: Claims 10-11 and 16-17 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Lendenmann in view of Beser.

a. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

Lendenmann recognizes the importance that data exchanged in the disclosed DCE system be able to utilize security measures to protect communications: "When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted." Lendenmann at 192.

Beser shows that one of the security measures that can be performed by the disclosed methods "is that of initiating and maintaining a virtual tunnel." Beser at 6:58-59. Beser emphasizes the importance of protecting the negotiation process in order to protect from hackers the identities of the originating and terminating telephony devices:

> The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90 address fields of the IP 58 packets that comprise the negotiation . . . . In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26). Beser at 12:6-19.

Additionally, Beser teaches that when anonymity is required, encryption can be used:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. Beser at 2:6-12.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by Beser would have been equally useful to those methods already described by Lendenmann.

Accordingly, Lendenmann in view of Beser would render obvious claim 10 of the '181 patent under 35 U.S.C. § 103.

b. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

Lendenmann recognizes the importance that data exchanged in the disclosed DCE system be able to utilize security measures to protect communications: "When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted." Lendenmann at 192.

Beser shows that one of the security measures that can be performed by the disclosed methods "is that of initiating and maintaining a virtual tunnel." Beser at 6:58-59. Beser emphasizes the importance of protecting the negotiation process in order to protect from hackers the identities of the originating and terminating telephony devices:

> The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90

> address fields of the IP 58 packets that comprise the negotiation. . . . In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26). Beser at 12:6-19.

Additionally, Beser teaches that when anonymity is required, encryption can be used:

> One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. Beser at 2:6-12.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by Beser would have been equally useful to those methods already described by Lendenmann.

Accordingly, Lendenmann in view of Beser would render obvious claim 11 of the '181 patent under 35 U.S.C. § 103.

c. Claim 16

Claim 16 depends from claim 15 and specifies "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof."

Beser also discloses a plurality of services and multimedia applications that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of incorporating various multimedia technologies disclosed by Beser would have been equally useful to those methods already described by Lendenmann.

Accordingly, Lendenmann in view of Beser would render obvious claim 16 of the '181 patent under 35 U.S.C. § 103.

d. Claim 17

Claim 17 depends from claim 15 and specifies "wherein the plurality of services comprises audio, video or a combination thereof."

Beser also discloses a plurality of services and multimedia applications that are able to utilize the disclosed secure communication links. For example:

> The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In 45 another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices. Beser at 4:43-54.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of incorporating various multimedia technologies disclosed by Beser would have been equally useful to those methods already described by Lendenmann.

Accordingly, Lendenmann in view of Beser would render obvious claim 17 of the '181 patent under 35 U.S.C. § 103.

4. Ground No. 8: Claims 10 and 11 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Lendenmann in view of RFC 2401.

a. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

Lendenmann recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted." Lendenmann at 192.

Generally, RFC 2401 is concerned with providing high quality security for Internet transactions that is adaptable to particular implementation needs and that facilitates interoperability over the Internet. *See, e.g.*, RFC 2401 at 4-5 ("The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations"; *see also Id.* at 5 ("A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.").

In particular, RFC 2401 defines the IPSec Protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes particular "cases" to implement secure communications involving a VPN, including "Case 3" which describes VPN implementation where edge routers on two different networks are used to establish an encrypted IP tunnel through which the network devices will communicate. RFC 2401 at 24-26.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by RFC 2401 would have been equally useful to those methods already described by Lendenmann.

Accordingly, Lendenmann in view of RFC 2401 would render obvious claim 10 of the '181 patent under 35 U.S.C. § 103.

b. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

Lendenmann recognizes the importance that data exchanged in the disclosed system utilize security measures to protect communications: "When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted." Lendenmann at 192.

Generally, RFC 2401 is concerned with providing high quality security for Internet transactions that is adaptable to particular implementation needs and that facilitates interoperability over the Internet. *See, e.g.*, RFC 2401 at 4-5 ("The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations"; *see also Id.* at 5 ("A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.").

In particular, RFC 2401 defines the IPSec Protocol, and provides a detailed explanation of how to implement a secure communication link in an IP tunneling model. In particular, RFC 2401 describes particular "cases" to implement secure communications involving a VPN, including "Case 3" which describes VPN implementation where edge routers on two different networks are used to establish an encrypted IP tunnel through which the network devices will communicate. RFC 2401 at 24-26.

A person skilled in the art before the effective filing date of the '181 patent would have immediately recognized the beneficial use of tunneling disclosed by RFC 2401 would have been equally useful to those security methods already described by Lendenmann.

Accordingly, Lendenmann in view of Beser would render obvious claim 11 of the '181 patent under 35 U.S.C. § 103.

VII. DETAILED EXPLANATION OF MANNER OF APPLYING PROVINO TO CLAIMS 1-29 AND PROPOSED REJECTIONS BASED ON GROUND NOS. 9-10.

Exhibit C4 correlates each of claims 1-23 and 28-29 of the '181 patent with the section of the present request that sets out the detailed basis for anticipation and/or obviousness of the claim, along with an identification of the relevant portions of Provino, alone or in conjunction with H.323. Requester notes that any emphasis indicated in quotations or other citations (e.g., as shown in bold faced text) has been added and is not original to the references cited in this section, unless otherwise noted.

A. Ground No. 9: Claims 1-23 and 28-29 are Unpatentable under 35 USC § 102(e) as Being Anticipated by Provino

Provino describes systems and methods for establishing secure communication links between devices connected to public networks such as the Internet through use of a secure DNS system that facilitates the resolution of human readable addresses. The DNS systems are illustrated in Figure 1 of Provino.

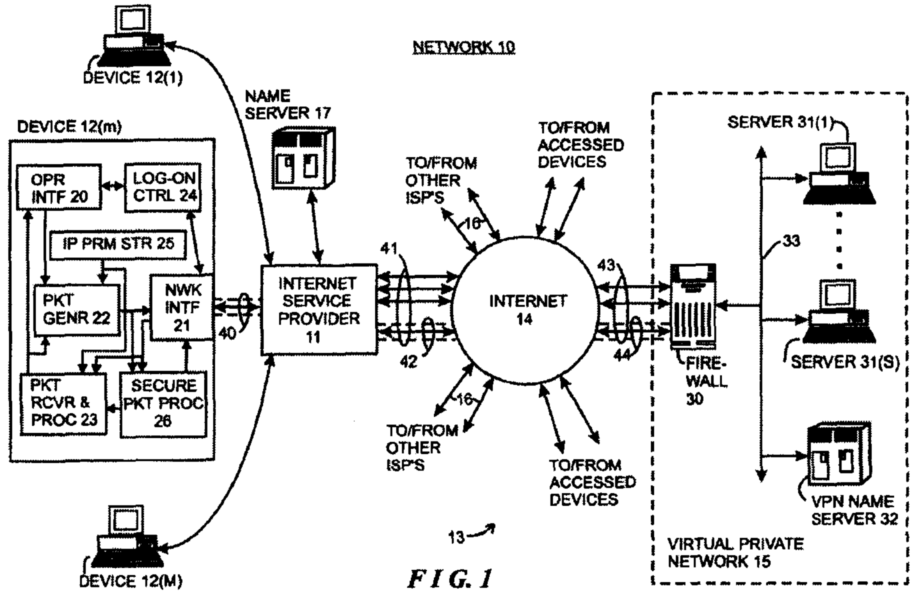


FIG. 1

Figure 1, *inter alia*, shows

(i) various devices (12(1) – 12(m)) interconnected for secure communication links through the Internet (14),

(ii) a Virtual Private Network (15) which is capable of secure communication to the other devices (15) through a firewall (30), and

(iii) name servers (17 and 32) that are capable of resolving the human readable domain names for integer Internet addresses and configured to establish

> secure communication links between the devices 12 as well as the actual secure communication link 15.

Each of these elements is then described in Provino, with guidance provided as to implementation of the functionality of each particular element, component or service.

Provino thus describes methods and systems for establishing a secure communication link between two devices across a public network such as the Internet.

1. Claim 1

Claim 1 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising":

> (a) receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and
>
> (b) sending a message over a secure communication link from the first device to the second device.

The preamble of claim 1 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name . . . ." As shown in Figure 1, provided above, Provino discloses two name servers, Name Server 17 and VPN Name Server 32. Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11:

> A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that name server 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Provino at 10:45-52.
>
> [I]n that connection the name server 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses. Provino at 9:2-5.

In Provino, the name servers are DNS servers:

> To accommodate the use of human-readable names, name servers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. Provino at 1:56-60.

Further, Provino teaches that for device 12(m) to reach server 31(s) in Virtual Private Network 15, it must first query public domain name server 17 to obtain an address for Firewall 30. The name stored in public domain name server 17 is an unsecured name, as described in the examples set forth below:

- In that operation, the packet generator 22 will initially contact name server 17 to attempt to obtain the appropriate integer Internet address from the name server 17. Provino at 8:40-43.

- Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device ....

  ***

  The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. Provino at 9:32-36, 52-56.

- [W]hen the device 12(m) and firewall 30 cooperate to establish a secure tunnel therebetween...the firewall 30 [] provides the device 12(m) with the identification of a name server, such as name server 32, in the virtual private network 15 which the device 12(m) can access to obtain the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m). Provino at 10:54-56, 62-67.

Device 12(m) is allowed access to Virtual Private Network 15 and server 31(s) only if it is authorized to do so. Device 12(m) may only establish a secure communication link upon receipt of the second device's secure name, i.e., the appropriate integer Internet address which is registered on VPN Name Server 32:

- If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15

> which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm and key that it...will use to the firewall 30 during the dialog. Provino at 9:56–10:7.

- If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). Provino at 9:17-27.

Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." *See* Provino at 8:67-9:5. Provino further describes that the secure DNS systems comprise secure domain names (e.g., the human-readable domain name associated with VPN 15 or like servers) that are "secure names" associated with secure communications. *See, e.g.*, Provino at 9: 32–10:13 (describing creation of "secure tunnel" between device 12(m) and VPN 15 through firewall 30). The secure nameservers within Provino (e.g., Nameserver 32 in Figure 1) thus can act on and resolve secure or private domain names that cannot be resolved through public or insecure nameservers.

Once the secure communication link is established, further DNS requests containing private domain names are routed to VPN Name Server 32 as follows:

> As noted above ... after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m) ... through the operator interface 20 ... provides a human-readable Internet address [i.e., a domain name], the device 12(m) ... will initially determine whether the IP parameter store 25 has cached therein an integer Internet address.... If not, the packet generator 22 will generate a request message packet for transfer to the name server 17 [i.e., the public DNS server] requesting it to provide the integer Internet address associated with the human-readable Internet address. If the name server 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.

> Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. Provino at 13:26-67.

Thus, Provino discloses "a non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name."

Step (a) of Claim 1 specifies: "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and"

Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12(m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52.

Thus, Provino discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Step (b) of claim 1 specifies: "sending a message over a secure communication link from the first device to the second device."

Provino further explains that its secure DNS system supports communications between devices over secure tunnels. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11.** A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical

> connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Thus, Provino discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Beser anticipates claim 1 of the '181 patent under 35 U.S.C. § 102(e).

2. Claim 2

Independent claim 2 is directed to "[a] method of using a first device to communicate with a second device having a secure name, the method comprising:

> (a) from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;
>
> (b) at the first device, receiving a message containing the network address associated with the secure name of the second device; and
>
> (c) from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

The preamble of claim 2 specifies "[a] method of using a first device to communicate with a second device having a secure name . . . ." As shown in Figure 1, provided above, Provino discloses two name servers, Name Server 17 and VPN Name Server 32. Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11:

> A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that name server 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Provino at 10:45-52.

> [I]n that connection the name server 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses. Provino at 9:2-5.

In Provino, the name servers are DNS servers:

> To accommodate the use of human-readable names, name servers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. Provino at 1:56-60.

Further, Provino teaches that for device 12(m) to reach server 31(s) in Virtual Private Network 15, it must first query public domain name server 17 to obtain an address for Firewall 30. Device 12(m) is allowed access to Virtual Private Network 15 and server 31(s) only if it is authorized to do so. Device 12(m) may only establish a secure communication link upon receipt of the second device's secure name, i.e., the appropriate integer Internet address which is registered on VPN Name Server 32:

- If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm and key that it...will use to the firewall 30 during the dialog. Provino at 9:56–10:7.

- If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). Provino at 9:17-27.

Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." *See* Provino at 8:67-9: 5. Provino describes secure DNS systems that comprise secure domain names (e.g., the human-readable domain name associated with VPN 15 or like servers) that are "secure names" associated with secure communications. *See, e.g.*, Provino at 9:32–10:13 (describing creation of "secure tunnel" between device 12(m) and VPN 15 through firewall 30).

Once the secure communication link is established, further DNS requests containing private domain names are routed to VPN Name Server 32 as follows:

> As noted above ... after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers

> 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m) ... through the operator interface 20 ... provides a human-readable Internet address [i.e., a domain name], the device 12(m) ... will initially determine whether the IP parameter store 25 has cached therein an integer Internet address.... If not, the packet generator 22 will generate a request message packet for transfer to the name server 17 [i.e., the public DNS server] requesting it to provide the integer Internet address associated with the human-readable Internet address. If the name server 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.
>
> Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. Provino at 13:26-67.

Thus, Provino discloses "[a] method of using a first device to communicate with a second device having a secure name."

Step (a) of claim 2 further specifies: "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Provino also shows that communications are generally initiated by a query initiated by the device or operator initiating the communication, and such query requests the network address associated with the secure name of the second device. For example, at 13:54-67, Provino generally explains that requests ("queries") are used in its secure DNS system as follows:

> Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). **Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that**

> **nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing**. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30.

Thus, Provino shows the step of "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Step (b) of claim 2 further specifies: "at the first device, receiving a message containing the network address associated with the secure name of the second device; and"

Provino also shows that the querying device receives a response message from name server 32 that comprises the network address associated with the secure name of the second device. For example, at 14:39-46, 57-63, Provino explains:

> After the name server 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the name server determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall.
>
> ***
>
> After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the name server 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet.

Thus, Provino shows the step of "at the first device, receiving a message containing the network address associated with the secure name of the second device; and."

Step (c) of claim 2 further specifies: "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the**

> **firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11.** A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Accordingly, Provino anticipates claim 2 of the '181 patent under 35 U.S.C. § 102(e).

3. Claim 3

Claim 3 depends from claim 2, and specifies "wherein the secure name of the second device is a secure domain name.

As described in more detail above, the name servers in Provino are Domain Name Servers (i.e., DNS servers) such that the secure name, which is registered with VPN Name Server 32, is a secure domain name, as explained in Provino, for example, at 1:56-60:

> To accommodate the use of human-readable names, name servers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses.

Accordingly, Provino anticipates claim 3 of the '181 patent under 35 U.S.C. § 102(e).

4. Claim 4

Claim 4 depends from claim 2, and specifies "wherein the secure name indicates security."

Name Server 17 responds to device 12(m)'s request to establish a secure communication link by providing an IP address known to Name Server 17 as the address associated with Firewall 30. For example:

> The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is ***known to and provided to the device 12(m) by the nameserver 17***. Provino at 9:32-36, 52-56.

As described above, the VPN server 32 resides behind firewall 30, such that the secure name obtained from VPN server 32 is known to indicate security.

Accordingly, Provino anticipates claim 4 of the '181 patent under 35 U.S.C. § 102(e).

5. Claim 5

Claim 5 of the '181 patent depends from claim 2, and specifies "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form."

Provino discloses secure DNS systems that use encryption. *See, e.g.*, Provino at 10:25-27, ("The secure packet processor 26, in turn encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key"); *Id.* at 9:60-10:13. Accordingly, Provino anticipates claim 28 under 35 U.S.C. § 102(e).

Accordingly, Provino anticipates claim 5 of the '181 patent under 35 U.S.C. § 102(e).

6. Claim 6

Claim 6 depends from claim 5, and specifies that the step of "further including decrypting the message."

Provino discloses secure DNS systems that use encryption. *See, e.g.*, Provino at 10:25-27, ("The secure packet processor 26, in turn encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key"); *Id.* at 9:60-10:13. It would have been inherent in Provino to "decrypt" the very information that it recommends encrypting.

Accordingly, Provino anticipates claim 6 of the '181 patent under 35 U.S.C. § 102(e).

7. Claim 7

Claim 7 of the '181 patent depends from claim 2, and specifies "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed."

The communication link established between device 12(m) and server 31(s) that passes within the secure tunnel can be a non-secure communication link. Similarly, the link between firewall 30 and server 31(s) can be a non-secure communication link. And, the link between the firewall and device 12(m) can be a secure communication link. Finally, the dialog between device 12(m) and firewall 30 before a secure tunnel is established can be a non-secure communication link. *See* Provino, at 9:32-52.

Accordingly, Provino renders claim 7 obvious in view of RFC 2401 under 35 U.S.C. § 103.

8. Claim 8

Claim 8 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

Provino also shows that the querying device receives a response message from VPN Name Server 32 that comprises the network address associated with the secure name of the second device. For example, at 14:39-46, 57-63, Provino explains:

> After the name server 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the name server determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall.
>
> ***
>
> After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the name server 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet.

Accordingly, Provino anticipates claim 8 of the '181 patent under 35 U.S.C. § 102(e).

9. Claim 9

Claim 9 depends from claim 2 and specifies that "further including automatically initiating the secure communication link after it is enabled."

The secure communication link disclosed in Provino is automatically initiated. *See, e.g.*, Provino at 9:46-10:7.

Accordingly, Provino anticipates claim 9 of the '181 patent under 35 U.S.C. § 102(e).

10. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

Provino also shows that the querying device receives a response message from VPN Name Server 32 that comprises the network address associated with the secure name of the second device, and further that the response message is sent through use of a secure tunnel. For example, at 14:39-46, 57-63, Provino explains:

> After the name server 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the name server determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall.
>
> ***

> After the firewall 30 receives the response message packet, **since communications with device 12(m) are over the secure tunnel therebetween,** it (that is, the firewall 30) will encrypt the response message packet received from the name server 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet.

Accordingly, Provino anticipates claim 10 of the '181 patent under 35 U.S.C. § 102(e).

11. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11.** A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Accordingly, Beser anticipates claim 11 of the '181 patent under 35 U.S.C. § 102(e).

12. Claim 12

Claim 12 depends from claim 2 and specifies "wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols."

The systems described by Provino provide a plurality of services and application programs through Internet communications. *See, e.g.*, Provino at 5:10-13, 28-32 (transfer of information over the Internet through "Web pages or the like"). Web pages inherently support a plurality of services, including audio applications and multimedia applications, as well as communication protocols.

Accordingly, Provino anticipates claim 12 of the '181 patent under 35 U.S.C. § 102(e).

13. Claim 13

Claim 13 depends from claim 2 and specifies "wherein the receiving and sending of messages through the secure communication link includes multiple sessions."

The systems described by Provino provide a plurality of services and application programs through Internet communications. *See, e.g.,* Provino at 5:10-13, 28-32 (transfer of information over the Internet through "Web pages or the like"). Web pages inherently support a plurality of services and multiple sessions, including audio applications and multimedia applications, as well as communication protocols.

Accordingly, Provino anticipates claim 13 of the '181 patent under 35 U.S.C. § 102(e).

14. Claim 14

Claim 14 depends from claim 2 and specifies "further including supporting a plurality of services over the secure communication link."

The systems described by Provino provide a plurality of services and application programs through Internet communications. *See, e.g.,* Provino at 5:10-13, 28-32 (transfer of information over the Internet through "Web pages or the like"). Web pages inherently support a plurality of services, including audio applications and multimedia applications, as well as communication protocols.

Accordingly, Provino anticipates claim 14 of the '181 patent under 35 U.S.C. § 102(e).

15. Claim 15

Claim 15 depends from claim 14 and specifies "wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof."

The systems described by Provino provide a plurality of services and application programs through Internet communications. *See, e.g.,* Provino at 5:10-13, 28-32 (transfer of information over the Internet through "Web pages or the like"). Web pages inherently support a plurality of services, including audio applications and multimedia applications, as well as communication protocols.

Accordingly, Provino anticipates claim 15 of the '181 patent under 35 U.S.C. § 102(e).

16. Claim 16

Claim 16 depends from claim 15 and specifies "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof."

The systems described by Provino provide a plurality of services and application programs through Internet communications. *See, e.g.,* Provino at 5:10-13, 28-32 (transfer of information over the Internet through "Web pages or the like"). Web pages inherently support a plurality of services and application programs, include video conferencing, email, wording process and telephony, along with other multimedia and audio applications.

Accordingly, Provino anticipates claim 16 of the '181 patent under 35 U.S.C. § 102(e).

17. Claim 17

Claim 17 depends from claim 15 and specifies "wherein the plurality of services comprises audio, video or a combination thereof."

The systems described by Provino provide a plurality of services and application programs through Internet communications. *See, e.g.,* Provino at 5:10-13, 28-32 (transfer of information over the Internet through "Web pages or the like"). Web pages inherently support a plurality of services, including audio, video and other multimedia and audio applications.

Accordingly, Provino anticipates claim 17 of the '181 patent under 35 U.S.C. § 102(e).

18. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

Provino further teaches secure DNS systems which authenticate requests ("queries") for network addresses using cryptographic techniques. Provino teaches systems that receive a query for a network address from the operator (and subsequently) from device 12(m). Provino at 9:46-60. This occurs during a dialog between the initiating and responding entities. For example, at 9:56-10:12, Provino explains:

> **During the dialog**, the firewall 30 may provide the device 12(m) with the identification of **a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m).** In addition, the firewall 30 may also provide the device 12(m) with the identification of **an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted**; alternatively, the device 12(m) can provide the identification of **the encryption algorithm and key that it (that is device 12(m)) will use to the firewall 30** during the dialog. The device 12(m) can store in its IP parameter store 25 information concerning the secure tunnel, including information associating the identification of the firewall 30 and the **identifications of the encryption and decryption algorithms and associated keys for message packets to be transferred over the secure tunnel.**

Accordingly, Provino anticipates claim 18 of the '181 patent under 35 U.S.C. § 102(e).

19. Claim 19

Claim 19 depends from claim 2 and specifies "wherein the first device is a computer, and the steps are performed on the computer."

Provino further discloses secure DNS systems in which a query is initiated from the first location (device 12(m)), and that the second location (e.g., VPN 15, which comprises device 13 and servers 31(s) comprises a computer. *See* Provino at 6:19-23 ("The firewall 30 and servers 31(s) maybe similar to any of the various devices of devices 12(m) and 13 and may include, for example, personal computers, computer workstations, and the like"). Provino also teaches network addresses associated with the firewall and devices, such as servers 31, within the VPN 15. *See, e.g.*, Provino at 9:52-65 and 10:45–11:25.

Accordingly, Provino anticipates claim 19 of the '181 patent under 35 U.S.C. § 102(e).

20. Claim 20

Claim 20 depends from claim 2 and specifies "wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network."

Provino further discloses secure DNS systems in which a query is initiated from the first location (device 12(m)), and that the second location (e.g., VPN 15, which comprises device 13 and servers 31(s) comprises a computer. *See* Provino at 6:19-23 ("The firewall 30 and servers 31(s) maybe similar to any of the various devices of devices 12(m) and 13 and may include, for example, personal computers, computer workstations, and the like"). Provino also teaches network addresses associated with the firewall and devices, such as servers 31, within the VPN 15. *See, e.g.*, Provino at 9:52-65 and 10:45–11:25.

Accordingly, Provino anticipates claim 20 of the '181 patent under 35 U.S.C. § 102(e).

21. Claim 21

Claim 21 depends from claim 2 and specifies "further including providing an unsecured name associated with the device."

As shown in Figure 1, provided above, Provino discloses two name servers, Name Server 17 and VPN Name Server 32. Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11

Accordingly, Provino anticipates claim 21 of the '181 patent under 35 U.S.C. § 102(e).

22. Claim 22

Claim 22 depends from claim 2 and specifies "wherein the secure name is registered prior to the step of sending a message to a secure name service."

As described above, VPN Name Server 32 stores the secure domain name for each of the servers that are the object of the desire to communicate. For the secure name to be resolved by VPN Server 32, it must have been previously registered.

Accordingly, Provino anticipates claim 22 of the '181 patent under 35 U.S.C. § 102(e).

23. Claim 23

Claim 23 depends from claim 2 and specifies "wherein the secure name of the second device is a secure, non-standard domain name."

As the secure name is only resolvable by VPN Name Server 32, and not Name Server 17, the secure name is a non-standard domain name.

Accordingly, Provino anticipates claim 23 of the '181 patent under 35 U.S.C. § 102(e).

24. Claim 28

Independent claim 28 is directed to "[a] non-transitory machine-readable medium comprising instructions for:

(a) sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

(b) receiving a message containing the network address associated with the secure name of the device; and

(c) sending a message to the network address associated with the secure name of the device using a secure communication link.

The preamble of claim 28 specifies "[a] non-transitory machine-readable medium comprising instructions." Provino discloses secure DNS systems in which a query is initiated from the first location (device 12(m)), and that the second location (e.g., VPN 15, which comprises device 13 and servers 31(s) comprises a computer. *See* Provino at 6:19-23 ("The firewall 30 and servers 31(s) maybe similar to any of the various devices of devices 12(m) and 13 and may include, for example, personal computers, computer workstations, and the like"). Provino also teaches network addresses associated with the firewall and devices, such as servers 31, within the VPN 15. *See, e.g.,* Provino at 9:52-65 and 10:45–11:25. Such communications would have been facilitated by, for example, machine-readable medium that comprises instructions.

Thus, Provino discloses [a] non-transitory machine-readable medium comprising instructions."

Step (a) of claim 28 further specifies: "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;"

Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12(m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52. Device 12(m) may only establish a secure communication link upon receipt of the second device's secure name, i.e., the appropriate integer Internet address which is registered on VPN Name Server 32. *See, e.g.,* Provino at 9:56–10:7.

Thus, Provino shows the step of "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

Step (b) of claim 28 further specifies: "receiving a message containing the network address associated with the secure name of the device; and"

Provino also shows that the querying device receives a response message from VPN Name Server 32 that comprises the network address associated with the secure name of the second device. For example, at 14:39-46, 57-63, Provino explains:

> After the name server 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the name server determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall.
>
> ***
>
> After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the name server 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet.

Step (c) of claim 28 further specifies: "sending a message to the network address associated with the secure name of the device using a secure communication link."

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11**. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical

> connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Thus, Provino discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Provino anticipates claim 28 of the '181 patent under 35 U.S.C. § 102(e).

25. Claim 29

Independent claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

(a) receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and

(b) sending a message securely from the first device to the second device.

The preamble of claim 29 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name . . . As shown in Figure 1, provided above, Provino discloses two name servers, Name Server 17 and VPN Name Server 32. Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11:

> A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that name server 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Provino at 10:45-52.
>
> [I]n that connection the name server 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses. Provino at 9:2-5.

In Provino, the name servers are DNS servers:

> To accommodate the use of human-readable names, name servers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. Provino at 1:56-60.

Further, Provino teaches that for device 12(m) to reach server 31(s) in Virtual Private Network 15, it must first query public domain name server 17 to obtain an address for Firewall 30. Device 12(m) is allowed access to Virtual Private Network 15 and server 31(s) only if it is authorized to do so. Device 12(m) may only establish a secure communication link upon receipt of the second device's secure name, i.e., the appropriate integer Internet address which is registered on VPN Name Server 32:

> - If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm and key that it...will use to the firewall 30 during the dialog. Provino at 9:56–10:7.
>
> - If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). Provino at 9:17-27.

Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." *See* Provino at 8:67-9:5. Provino describes secure DNS systems that comprise secure domain names (e.g., the human-readable domain name associated with VPN 15 or like servers) that are "secure names" associated with secure communications. *See, e.g.*, Provino at 9:32–10:13 (describing creation of "secure tunnel" between device 12(m) and VPN 15 through firewall 30).

Once the secure communication link is established, further DNS requests containing private domain names are routed to VPN Name Server 32 as follows:

> As noted above ... after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers

> 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m) … through the operator interface 20 … provides a human-readable Internet address [i.e., a domain name], the device 12(m) … will initially determine whether the IP parameter store 25 has cached therein an integer Internet address…. If not, the packet generator 22 will generate a request message packet for transfer to the name server 17 [i.e., the public DNS server] requesting it to provide the integer Internet address associated with the human-readable Internet address. If the name server 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.
>
> Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. Provino at 13:26-67.

Thus, Provino discloses "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name…"

Step (a) of claim 29 further specifies: "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and"

Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12(m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52. Device 12(m) may only establish a secure communication link upon receipt of the second device's secure name, i.e., the appropriate integer Internet address which is registered on VPN Name Server 32. *See, e.g.,* Provino at 9:56–10:7.

Thus, Provino shows the step of "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered."

Step (b) of claim 29 further specifies: "sending a message securely from the first device to the second device."

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11**. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Thus, Provino discloses "sending a message over a secure communication link from the first device to the second device."

Accordingly, Provino anticipates claim 29 of the '181 patent under 35 U.S.C. § 102(e).

B. Ground No. 10: Claims 24-26 would have been obvious to a person of ordinary skill under 35 U.S.C. § 103 based on Provino in view of H.323.

1. Relevant Teachings of the Primary Reference (Provino)

A detailed explanation of Provino is provided in §§ **VII.A.**

2. Relevant Teachings of the Secondary Reference (H.323)

A detailed explanation of H.323 is provided in §§ **VIII.A.**

3. Claim 24

Independent claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network, the method comprising:

> (a) at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;
>
> (b) receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and
>
> (c) sending a message securely from the first device to the second device."

The preamble of claim 24 specifies "[a] method of using a first device to securely communicate with a second device over a communication network . . . ." As shown in Figure 1, provided above, Provino discloses two name servers, Name Server 17 and VPN Name Server 32. Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11:

> A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that name server 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Provino at 10:45-52.
>
> [I]n that connection the name server 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses. Provino at 9:2-5.

In Provino, the name servers are DNS servers:

> To accommodate the use of human-readable names, name servers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. Provino at 1:56-60.

Further, Provino teaches that for device 12(m) to reach server 31(s) in Virtual Private Network 15, it must first query public domain name server 17 to obtain an address for Firewall 30. Device 12(m) is allowed access to Virtual Private Network 15 and server 31(s) only if it is authorized to do so. Device 12(m) may only establish a secure communication link upon receipt of the second device's secure name, i.e., the appropriate integer Internet address which is registered on VPN Name Server 32:

> - If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may

also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm and key that it...will use to the firewall 30 during the dialog. Provino at 9:56–10:7.

- If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). Provino at 9:17-27.

Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." *See* Provino at 8:67-9:5. Provino describes secure DNS systems that comprise secure domain names (e.g., the human-readable domain name associated with VPN 15 or like servers) that are "secure names" associated with secure communications. *See, e.g.*, Provino at 9:32-10:13 (describing creation of "secure tunnel" between device 12(m) and VPN 15 through firewall 30).

Once the secure communication link is established, further DNS requests containing private domain names are routed to VPN Name Server 32 as follows:

As noted above ... after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m) ... through the operator interface 20 ... provides a human-readable Internet address [i.e., a domain name], the device 12(m) ... will initially determine whether the IP parameter store 25 has cached therein an integer Internet address.... If not, the packet generator 22 will generate a request message packet for transfer to the name server 17 [i.e., the public DNS server] requesting it to provide the integer Internet address associated with the human-readable Internet address. If the name server 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.

Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. Provino at 13:26-67.

Thus, Provino discloses "[a] method of using a first device to securely communicate with a second device over a communication network."

Step (a) of claim 24 further specifies: "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

It would have been obvious for a person of ordinary skill to combine the teachings of H.323 and its related protocols given its global reach and its applicability to communicating via secure communication links between two devices. The H.323 recommendation discloses a system whereby each communicating device on a network can request and obtain registration of a secure name for the device, called an "Alias Address," which is associated with a network address. The Alias address can, for example, be an email address or an alphanumeric string in the form of an email address:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Alias addresses are resolved into network addresses, such as IP addresses, by a Gatekeeper computer. The Gatekeeper provides a number of services, including address translation:

> Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed. H.323 at 27.

Transport Addresses are IP addresses in packet-based networks utilizing TCP/IP:

> **3.42 transport address**: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the ***Network Address*** plus the TSAP identifier [port number] of the addressable H.323 entity.
>
> **3.33 network address**: The network layer address of an H.323 entity as defined by the (inter)network layer protocol in use (e.g. an IP address). This address is mapped onto the

> layer one address of the respective system by some means defined in the (inter)networking protocol. H.323 at 7-8.

The endpoints of the H.323 recommendation, i.e., the devices desiring to securely communicate, may register their Alias and transport addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Further, "endpoints" may register "one or more alias addresses associated with it." H.323 at 33.

In the H.323 recommendation, "Alias Address" can constitute "secure names" because, for example, they can be protected by "access tokens," which have the function of ensuring the anonymity of an endpoint's Transport Address and Alia Address:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.

The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38.

Step (b) of claim 24 further specifies: "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and."

Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12(m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52.

Thus, Provino shows the step of "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device."

Step (c) of claim 24 further specifies: "sending a message securely from the first device to the second device.

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11**. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Accordingly, Provino in view of H.323 would have rendered claim 24 of the '181 patent obvious under 35 U.S.C. § 103.

4. Claim 25

Claim 25 depends from claim 24 and specifies "wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link."

As described above, it would have been obvious to one of ordinary skill in the art to utilize the "secure name" registration process described in H.323, which would have entailed registering a "secure name" with a first device utilizing a first device.

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino at 9:32-44. As Provino explains:

> Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be**

maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Accordingly, Provino in view of H.323 would have rendered claim 25 of the '181 patent obvious under 35 U.S.C. § 103.

5. Claim 26

Independent claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising:

(a) from the first device requesting and obtaining registration of an unsecured name associated with the first device;

(b) from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;

(c) receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

(d) from the first device sending a message securely from the first device to the second device."

The preamble of claim 26 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name . . . As described in the ABSTRACT:

> A system [comprises] includes a virtual private network and an external device interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the

> nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.

Thus, Provino discloses "[a] method of using a first device to communicate with a second device over a communication network ..."

Step (a) of claim 26 further specifies: "from the first device requesting and obtaining registration of an unsecured name associated with the first device"

Provino in view of H.323 thus discloses "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

It would have been obvious for a person of ordinary skill to combine the teachings of H.323 and its related protocols given its global reach and its applicability to communicating via secure communication links between two devices. The H.323 recommendation discloses a system whereby each communicating device on a network can request and obtain registration of a secure name for the device, called an "Alias Address," which is associated with a network address. The Alias address can, for example, be an email address or an alphanumeric string in the form of an email address:

> 7.1.3 Alias address
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Alias addresses are resolved into network addresses, such as IP addresses, by a Gatekeeper computer. The Gatekeeper provides a number of services, including address translation:

> Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed. H.323 at 27.

Transport Addresses are IP addresses in packet-based networks utilizing TCP/IP:

> **3.42 transport address**: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the ***Network Address*** plus the TSAP identifier [port number] of the addressable H.323 entity.

> **3.33 network address**: The network layer address of an H.323 entity as defined by the (inter)network layer protocol in use (e.g. an IP address). This address is mapped onto the layer one address of the respective system by some means defined in the (inter)networking protocol. H.323 at 7-8.

The endpoints of the H.323 recommendation, i.e., the devices desiring to securely communicate, may register their Alias and transport addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Further, "endpoints" may register "one or more alias addresses associated with it." H.323 at 33.

In the H.323 recommendation, "Alias Address" can constitute "secure names" because, for example, they can be protected by "access tokens," which have the function of ensuring the anonymity of an endpoint's Transport Address and Alia Address:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.

The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38.

Step (b) of claim 26 further specifies: "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device"

As disclosed in the H.323 recommendation, each communicating device on a network can request and obtain registration of a secure name for the device, called an Alias Address, which is associated with a network address. The Alias address can, e.g., be an email address or an alphanumeric string in the form of an email address:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Alias addresses are resolved into network addresses, such as IP addresses, by a Gatekeeper computer:

> When it is present in a system, the Gatekeeper shall provide the following services:
>
> - Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed. H.323 at 27.

In the H.323 recommendation, Transport Addresses are IP addresses in packet-based networks utilizing TCP/IP:

> **3.42 transport address**: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the ***Network Address*** plus the TSAP identifier [port number] of the addressable H.323 entity.
>
> **3.33 network address**: The network layer address of an H.323 entity as defined by the (inter)network layer protocol in use (e.g. an IP address). This address is mapped onto the layer one address of the respective system by some means defined in the (inter)networking protocol. H.323 at 7-8.

The endpoints of the H.323 recommendation, i.e., the devices desiring to securely communicate, may register their Alias and transport addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Further, "endpoints" may register "one or more alias addresses associated with it." H.323 at 33.

In the H.323 recommendation, "Alias Address" can constitute "secure names" because, for example, they can be protected by "access tokens," which have the function of ensuring the anonymity of an endpoint's Transport Address and Alia Address:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38.

Step (c) of claim 26 further specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and"

H.323 expressly references the authentication and security services that are described in H.235. Although "authentication and security for H.323 systems is optional," if it is provided, "it shall be provided in accordance with Recommendation H.235." H.323 at 81.

The Access tokens have two uses in the H.323 recommendation: to shield an endpoint's alias name and transport address, when desired, and to ensure that a calling endpoint can access the called endpoint directly:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.

> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 in 38.

As described in H.235, IPSec can then be used to secure communications between the two endpoints:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> 3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the

> initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. H.235 at 30-31.

See also, H.235 at 6, which describes call establishment security call control security, and media stream privacy, in which all communications are secure.

Step (d) of claim 26 further specifies: "from the first device sending a message securely from the first device to the second device."

It would have been obvious for a person of ordinary skill to combine the teachings of H.323 and its related protocols given its global reach and its applicability to communicating via secure communication links between two devices. The H.235 protocol of the H.323 recommendation describes call establishment security, call control security, and media stream privacy, in which all communications are sent securely. H.235 at 6. For example:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.
>
> **6.4 Call control (H.245) security**
>
> The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.
>
> The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel

> is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this.
>
> **6.5 Media stream privacy**
>
> This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. H.235 at 6.

Provino in view of H.323 thus discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Step (c) of claim 26 further specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and"

Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12(m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52.

Thus, Provino shows the step of "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device."

Step (d) of claim 26 further specifies: "from the first device sending a message securely from the first device to the second device."

Provino further explains that its secure DNS system supports communications between devices over secure tunnels, which communications are established by sending a message to the network address associated with the secure name of the second device. *See, e.g.*, Provino, at 9:32-44. As Provino explains:

Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, **may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11**. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Thus, Provino discloses "from the first device sending a message securely from the first device to the second device."

Accordingly, Provino in view of H.323 would have rendered claim 26 of the '181 patent obvious under 35 U.S.C. § 103.

6. Claim 27

Claim 27 depends from claim 26 and specifies:

(a) "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

(b) wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Step (a) of claim 27 specifies: "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

It would have been obvious for a person of ordinary skill to combine the teachings of H.323 and its related protocols given its global reach and its applicability to communicating via secure communication links between two devices.

As indicated above, all H.323 endpoints register their aliases:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Step (b) of claim 27 specifies: wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

It would have been obvious for a person of ordinary skill to combine the teachings of H.323 and its related protocols given its global reach and its applicability to communicating via secure communication links between two devices.

As indicated above, all H.323 endpoints register their aliases:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Endpoints register their Access Tokens for secure names:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. ***The Gatekeeper will know the endpoint related to the Access Token from the registration process***.... H.323 at 38.

Accordingly, Provino in view of H.323 would have rendered claim 27 of the '181 patent obvious under 35 U.S.C. § 103.

VIII. Detailed Explanation of Applying H.323 to Claims 1-29 and Proposed Rejections Based on Ground Nos. 11-12.

Exhibit C5 correlates each of claims 1-29 of the '181 patent with the section of the present request that sets out the detailed basis for anticipation and/or obviousness of the claim, along with an identification of the relevant portions of H.323. Requester notes that any emphasis indicated in quotations or other citations (e.g., as shown in bold faced text) has been added and is not original to the references cited in this section, unless otherwise noted.

A. Ground No. 11: Claims 1-29 are Unpatentable under 35 USC § 102(b) as Being Anticipated by H.323

The Telecommunication Sector of the International Telecommunication Union (ITU-T) developed a series of recommendations together comprising the H.323 system, which provides for secure multimedia communications in packet-based networks. The H.323 recommendation includes the teaching and disclosure of H.225.0, "core message definitions," H.235, "security framework," and H.245, "media channel control." These series of recommendations are incorporated by reference because they are specifically referenced and described as disclosing particular features of the H.323 recommendation.

H.323 expressly incorporates Recommendations H.225.0 ("Call signaling protocols and media stream packetization for packet based multimedia communication systems"), H.245 ("Control protocol for multimedia communication"), and H.235 ("Security and encryption for H-Series (H.323 and other H.245 based) multimedia terminals"):

> **2 Normative references**
>
> The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation.
>
> [1] ITU-T Recommendation H.225.0 (1998), Call signaling protocols and media stream packetization for packet based multimedia communication systems.
>
> [2] ITU-T Recommendation H.245 (1998), Control protocol for multimedia communication.
>
> ***
>
> [22] ITU-T Recommendation H.235 (1998), Security and encryption for H-Series (H.323 and other H.245 based) multimedia terminals. H.323 at 2-3.

H.323 expressly references the authentication and security services of H.235:

> **10.1 Encryption**
>
> Authentication and security for H.323 systems is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235. H.323 at 81.

H.323 expressly references Recommendations H.225.0 and H.245:

> Products claiming compliance with Version 1 of H.323 shall comply with all of the mandatory requirements of H.323 (1996) which references Recommendations H.225.0 (1996) and H.245 (1996). Version 1 products can be identified by H.225.0 messages containing a protocolIdentifier = {itu-t (0) recommendation (0) h (8) 2250 version (0) 1} and H.245 messages containing a protocolIdentifier = {itu-t (0) recommendation (0) h (8) 245 version (0) 2}. Products claiming compliance with Version 2 of H.323 shall comply with all of the mandatory requirements of this Recommendation, H.323 (1998), which references Recommendations H.225.0 (1998) and H.245 (1998). H.323 at (i).

Any reference below to H.225 is a reference to Recommendation H.225.0 for simplicity.

H.323 relates to terminals and other entities that provide multimedia communications services over packet-based networks (PBN), such as the Internet:

> This Recommendation describes terminals and other entities that provide multimedia communications services over Packet Based Networks (PBN) which may not provide a guaranteed Quality of Service. H.323 entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork.
>
> ***
>
> This Recommendation describes terminals and other entities that provide multimedia communications services over Packet Based Networks (PBN) which may not provide a guaranteed Quality of Service. H.323 entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork. H.323 at (i).
>
> These packet based networks may include Local Area Networks, Enterprise Area Networks, Metropolitan Area Networks, Intra-Networks, and Inter- Networks (including the Internet). H.323 at 1.

An H.323 terminal is an endpoint on a network that provides for real-time communications and includes Gateways and Multipoint Control Units (MCU):

> **3.41 terminal**: An H.323 Terminal is an endpoint on the network which provides for real-time, two-way communications with another H.323 terminal, Gateway, or Multipoint Control Unit. This communication consists of control, indications, audio, moving colour video pictures, and/or data between the two terminals. A terminal may provide speech only, speech and data, speech and video, or speech, data and video. H.323 at 8.

A Gateway is an endpoint on a packet-based network that connects the packet-based network to a circuit-switched network where other ITU Terminals (endpoints) reside, or to another H.323 Gateway:

> **3.16 gateway**: An H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 Terminals on the packet based network and other ITU Terminals on a switched circuit network, or to another H.323 Gateway. Other ITU Terminals include those complying with Recommendations H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.324 (GSTN), H.324M (Mobile), and V.70 (DSVD). H.323 at 5.

H.323 includes a Gatekeeper that performs address translation (i.e., name resolution):

> **3.15 gatekeeper**: The Gatekeeper (GK) is an H.323 entity on the network that provides address translation and controls access to the network for H.323 terminals, Gateways and MCUs. The Gatekeeper may also provide other services to the terminals, Gateways and MCUs such as bandwidth management and locating Gateways. H.323 at 5.
>
> When it is present in a system, the Gatekeeper shall provide the following services:
>
> - **Address Translation** – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed.
>
> - **Admissions Control** – The Gatekeeper shall authorize network access using ARQ/ACF/ARJ H.225.0 messages. This may be based on call authorization, bandwidth, or some other criteria which is left to the manufacturer. It may also be a null function which admits all requests.
>
> ***
>
> - **Zone Management** – The Gatekeeper shall provide the above functions for terminals, MCUs, and Gateways which have registered with it as described in 7.2.

Authentication and security are provided through H.235:

> **10.1 Encryption**
>
> Authentication and security for H.323 systems is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235. H.323 at 81.

Authentication and security includes call establishment security, call control security, media stream privacy, and use of certificates to establish secure channels:

> **6.2.1 Certificates**
>
> The standardization of certificates, including their generation, administration and distribution is outside the scope of this Recommendation. The certificates used to establish secure channels (call signaling and/or call control) shall conform to those prescribed by whichever protocol has been negotiated to secure the channel.

It should be noted that for authentication utilizing public key certificates, the endpoints are required to provide digital signatures using the associated private key value. The exchange of public key certificates alone does not protect against man-in-the-middle attacks. The H.235 protocols conform to this requirement.

6.3 Call establishment security

There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.

6.4 Call control (H.245) security

The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.

The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this.

6.5 Media stream privacy

This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating endpoints may utilize an encrypted H.245 channel. In this manner, cryptographic algorithm selection and encryption keys as passed in the H.245 OpenLogicalChannel command are protected.

> The H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy. This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity. H.235 at 6.

In sum, H.323 discloses a system for securely communicating between two devices over a packet-based communication network, such as the Internet. The disclosed system utilizes secure and unsecured names in order to facility secure communications between two participating devices. H.323 thus provides a new and relevant disclosure in view of those references already considered by the Office.

Citations below may reference one or more of the Recommendations.

1. Claim 1

Claim 1 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising":

(a) receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and

(b) sending a message over a secure communication link from the first device to the second device.

The preamble of claim 1 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name...." Each device in H.323 network will include a non-transitory machine readable (e.g., a storage device) which is comprises executable code (e.g., "instructions") that enable the device to communicate with a first associated with a secure name and an unsecured name. In the case of H.323 devices, each device is associated with one or more alias names, called Alias Addresses, which can be in the form of a phone number or an email address:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

An Alias address can also be a user or conference name or other identifier:

> The H.323 ID consists of a string of ISO/IEC 10646-1 characters as defined in Recommendation H.225.0. It may be a user name, conference name, e-mail name, or other identifier.
>
> An endpoint may have more than one alias address (including more than one of the same type) which is translated to the same Transport Address. The endpoint's alias addresses shall be unique within a Zone. H.323 at 34.

Alias Addresses can be "secure names" because, among other reasons, they can be protected by "access tokens," which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38.

Alias addresses are resolved into network addresses, such as IP addresses, by the Gatekeeper computer. The Gatekeeper provides a number of services, including address translation:

> Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed. H.323 at 27.

Transport Addresses are IP addresses in packet-based networks utilizing TCP/IP:

> **3.42 transport address**: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the ***Network Address*** plus the TSAP identifier [port number] of the addressable H.323 entity.

> **3.33 network address**: The network layer address of an H.323 entity as defined by the (inter)network layer protocol in use (e.g. an IP address). This address is mapped onto the layer one address of the respective system by some means defined in the (inter)networking protocol. H.323 at 7-8.

Endpoints can register more than one Alias address with a Gatekeeper:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and ***alias addresses***. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint powerup). H.323 at 35.

H.323 teaches that one could register an unsecured name and a secure name for a single device. For example, a single endpoint may have multiple aliases, including an alias that represents the endpoint and an alias that may represent conferences the endpoint hosts, as indicated above.

Alternatively, endpoints can register a secure name and be associated with the unsecured names of the Gatekeeper computer with which they are registered. For example, endpoints issue a Registration Request (RRQ) to a Gatekeeper to register its aliases and the Gatekeeper responds with a Registration Confirmation (RCF):

> An endpoint shall send a Registration Request (RRQ) to a Gatekeeper. This is sent to the Gatekeeper's RAS Channel Transport Address. The endpoint has the Network Address of the Gatekeeper from the Gatekeeper discovery process and uses the well-known RAS Channel TSAP Identifier. The Gatekeeper shall respond with either a Registration Confirmation (RCF) or a Registration Reject (RRJ). H.323 at 35

Gatekeepers have unsecured names registered in the public DNS:

> **IV.1.1.2 Discovery using DNS (informative)**
>
> **IV.1.1.2.1 A URL for gatekeepers**
>
> As a first step, note that a gatekeeper is identified by a transport address and a gatekeeperIdentifier, which is a string. A gatekeeper is a particular resource on the Internet, so it is reasonable to specify it in a Uniform Resource Locator (URL). The

> protocol spoken by the gatekeeper is RAS, so the URL for a gatekeeper could be given by:
>
> ras://gkID@domainname
>
> gkID is the gatekeeperIdentifier, and domainname is a DNS domain name which identifies the gatekeeper's domain. Note that this is not necessarily a Fully Qualified Domain Name (FQDN) with an A-record – it is not required that this domain name has a physical transport interface with an IP number recorded in the DNS. If it is a FQDN, however, it is reasonable to insist that its IP number is that of the gatekeeper to which the URL refers. In this case, it is allowed to add an optional port number to the URL:
>
> ras://gkID@domainname:port_no.
>
> If no port number is given, then the well known value of 1719 is taken as a default.
>
> The more interesting case is when this is not an FQDN, and then the domain name does not refer to a transport address listed in the DNS. The domain name then can refer to a pure "gatekeeper zone of authority". The next subclause explains how to find the gatekeeper in this case. H.225 at 141.

See also, H.225 at 141-143, describing use of the DNS TXT and DNS SRV Resource Records in the public, Internet domain name system for locating the proper Gatekeeper computer on which a particular H.323 terminal is registered. The name corresponding to Gatekeeper computer for the H.323 endpoint is an unsecured name associated with the endpoint.

In other words, each endpoint can register a secure name with its Gatekeeper and be located on the Internet using the domain name associated with the endpoint in the public DNS, which identifies the endpoint's Gatekeeper computer.

Alternatively, MCUs and Gateways are endpoints and register multiple Alias names, as well:

> **3.14 endpoint**: An H.323 terminal, ***Gateway***, or MCU. An endpoint can call and be called. It generates and/or terminates information streams. H.323 at 5.
>
> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. H.323 at 33.

A Gateway is an endpoint on a packet-based network that connects the packet-based network to a circuit-switched network where other ITU Terminals (endpoints) reside, or to another H.323 Gateway:

> **3.16 gateway**: An H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 Terminals on the packet based network and other ITU Terminals on a switched circuit network, or to another H.323 Gateway. Other ITU Terminals include those complying with Recommendations H.310

> (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.324 (GSTN), H.324M (Mobile), and V.70 (DSVD). H.323 at 5.

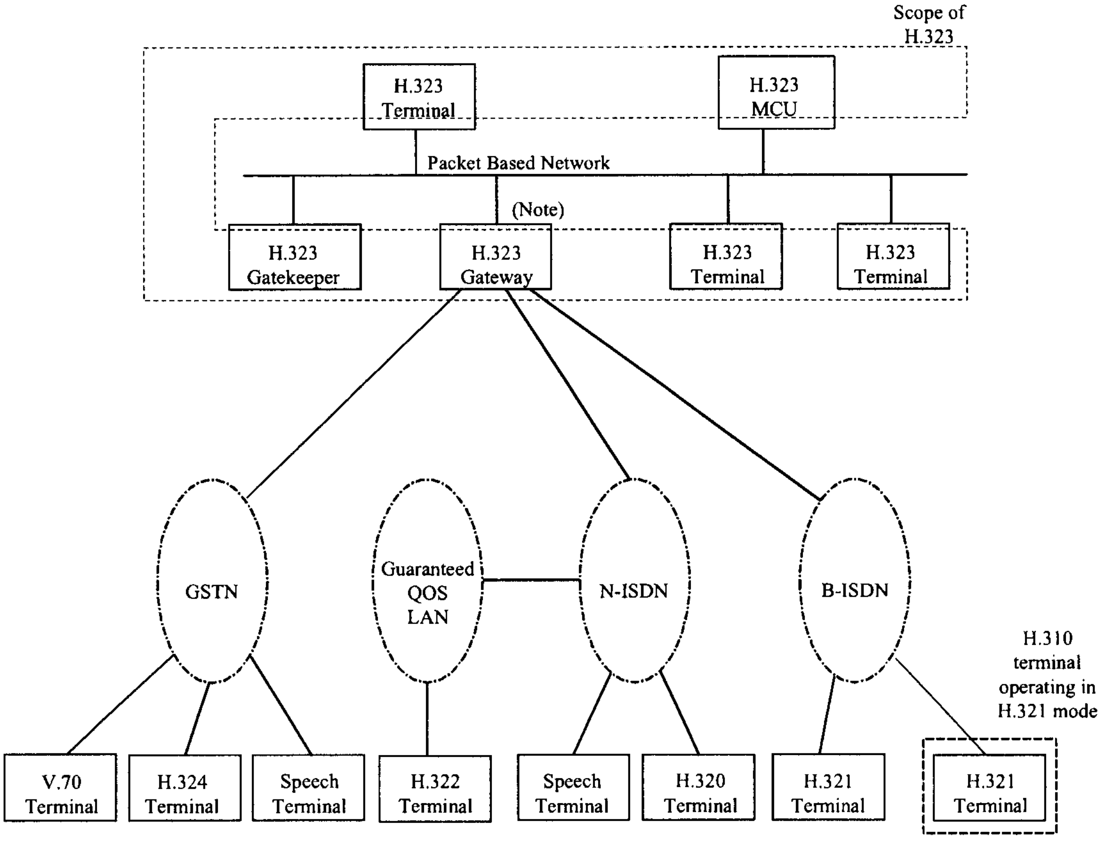
Gateways and MCUs may register two or more Transport Addresses for each Alias address:

> A Gateway or MCU may register a single Transport Address or multiple Transport Addresses. The use of multiple Transport Addresses may simplify the routing of calls to specific ports. H.323 at 35.

A single Gateway may terminate calls to multiple Switched Circuit Network (SCN) endpoints:

> **3.7 call**: Point-to-point multimedia communication between two H.323 endpoints. The call begins with the call set-up procedure and ends with the call termination procedure. The call consists of the collection of reliable and unreliable channels between the endpoints. A call may be directly between two endpoints, or may include other H.323 entities such as a Gatekeeper or MC. ***In case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway*** where they are converted to the appropriate representation for the SCN end system. Typically, a call is between two users for the purpose of communication, but may include signaling-only calls. An endpoint may be capable of supporting multiple simultaneous calls. H.323 at 5-6.

See also, Figure 1 below (H.323 at 2) showing an H.323 Gateway connecting multiple SCN devices to the packet-based network via different switched circuit networks (SCNs):



NOTE – A gateway may support one or more of the GSTN, N-ISDN and/or B-ISDN connections.

As indicated SCN means "Switched Circuit Network" and includes GSTN, N-ISDN, and B-ISDN networks:

> **3.40 Switched Circuit Network (SCN)**: A public or private switched telecommunications network such as the GSTN, N-ISDN, or B-ISDN.
>
> NOTE – While B-ISDN is not strictly a switched circuit network, it exhibits some of the characteristics of an SCN through the use of virtual circuits.

Thus, each H.323 endpoint is associated with both a secure name (i.e., Access Token) and an unsecured name (i.e., either another Alias name, the name in the DNS system for locating the Gatekeeper computer in which it is registered, or for a Gateway endpoint, two devices obtaining access to the packet-based network through the Gateway, one having a secure name and the other an unsecured name).

Step (a) of Claim 1 specifies: "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and"

An H.323 endpoint registers an Access Token instead of a regular Alias address with the Gatekeeper to secure its name and to receive communications at the network address associated with the secure name:

> ### 7.2.5 Access tokens
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly. H.323 at 38.

See also the following example using security tokens and a Gateway to reach a POTS-B device:

> This subclause will describe an example usage of security tokens to obscure or hide destination addressing information. The example scenario is an endpoint which wishes to make a call to another endpoint utilizing its well-known alias. More specifically, this involves an H.323 endpoint, gatekeeper, POTS-gateway, and telephone as illustrated below.

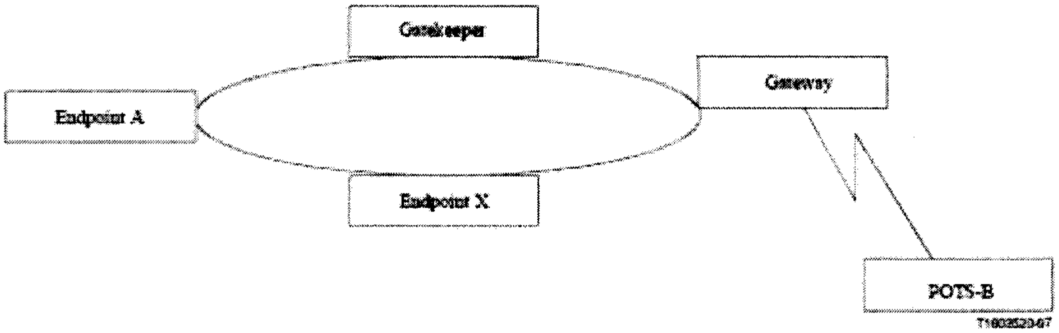


Figure I.6/H.235

> Assume that EPA [Endpoint A] is trying to call POTS-B, and POTS-B does not want to expose its E.164 phone number to EPA.
>
> - EPA will send an ARQ to its gatekeeper to resolve the address of the POTS telephone as represented by its alias/GW. The gatekeeper would recognize this as a "private" alias, knowing that in order to complete the connection it must return the POTS-gateway address (similar to returning the address of an H.320 gateway if an H.320 endpoint is called by an H.323 endpoint).

> - In the returned ACF, the gatekeeper returns the POTS-gateway's address as expected. The addressing information that is required to dial to the end telephone (i.e. the telephone number) is returned in an encrypted token included in the ACF. This encrypted token contains the actual E.164 (phone number) of the telephone which cannot be deciphered nor understood by the caller (i.e. EPA).
>
> - The endpoint issues the SETUP message to the gateway device (whose call signaling address was returned in the ACF) including the opaque token(s) that it received with the ACF.
>
> - The gateway, upon receiving the SETUP, issues its ARQ to its gatekeeper, including any token(s) that were received in the SETUP.
>
> - The gatekeeper is able to decipher the token(s) and return the phone number in the ACF. H.235 at 28-29.

The second device sends a message to the first device of the desire to communicate securely by, e.g., coordinating an IPSec setup with its Gatekeeper or by negotiating security with the endpoint itself:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint [second device] and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.

> 3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. Because the H.245 protocol is defined for the master to distribute the media keying material on the H.245 channel (to allow for multipoint communication), it is not recommended that IPSEC be used for the RTP channel.
>
> *See* H.235 at 30-31.

Security from the second device to the first device includes call establishment security, call control security, and media stream privacy, all include a message from the second device sent to the first device of the desire to securely communicate:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.
>
> **6.4 Call control (H.245) security**
>
> The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the

conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.

The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this. H.235 at 6.

6.5 Media stream privacy

This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating endpoints may utilize an encrypted H.245 channel. In this manner, cryptographic algorithm selection and encryption keys as passed in the H.245 OpenLogicalChannel command are protected.

The H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy. This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity.

If it is required that the H.245 channel be operated in a non-encrypted manner, the specific media encryption keys may be encrypted separately in the manner signaled and agreed to by the participating parties. A logical channel of type h235Control may be utilized to provide the material to protect the media encryption keys. This logical channel may be operated in any appropriately negotiated mode.

The privacy (encryption) of data carried in logical channels shall be in the form specified by the OpenLogicalChannel. Transport-specific header information shall not be encrypted. The privacy of data is to be based upon end-to-end encryption. H.235 at 6-7.

Step (b) of claim 1 specifies: "sending a message over a secure communication link from the first device to the second device."

The result of step (a) above is sending a message over a secure communication link from the first device to the second device by, e.g., using media stream privacy or the any of the security measures discussed in step (a) above.

Accordingly, H.323 anticipates claim 1 of the '181 patent under 35 U.S.C. § 102(b) above.

2. Claim 2

Independent claim 2 is directed to [a] method of using a first device to communicate with a second device having a secure name, the method comprising:

(a) from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;

(b) at the first device, receiving a message containing the network address associated with the secure name of the second device; and

(c) from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

Step (a) of claim 2 further specifies: "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

In H.323, Gatekeepers are a secure name service. For example, Gatekeepers perform network address translation and admission control, i.e., authorize access to the network for the endpoints in the Gatekeepers Zone:

> When it is present in a system, the Gatekeeper shall provide the following services:
>
> - Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed.
>
> - Admissions Control – The Gatekeeper shall authorize network access using ARQ/ACF/ARJ H.225.0 messages. This may be based on call authorization, bandwidth, or some other criteria which is left to the manufacturer. It may also be a null function which admits all requests.
>
> - Zone Management – The Gatekeeper shall provide the above functions for terminals, MCUs, and Gateways which have registered with it as described in 7.2. H.323 at 27.
>
> **3.49 zone**: A Zone (see Figure 3) is the collection of all terminals (Tx), Gateways (GW), and Multipoint Control Units (MCUs) managed by a single Gatekeeper (GK). A Zone includes at least one terminal, and may or may not include Gateways or MCUs. A Zone has one and only one Gatekeeper. A Zone may be independent of network topology and may be comprised of multiple network segments which are connected using routes (R) or other devices. H.323 at 8.

Gatekeepers implement call authorization, restricting access to certain terminals or gateways:

> Call Authorization – Through the use of the H.225.0 signaling, the Gatekeeper may reject calls from a terminal due to authorization failure. The reasons for rejection may include, but are not limited to, restricted access to/from particular terminals or Gateways, and restricted access during certain periods of time. The criteria for determining if authorization passes or fails is outside the scope of this Recommendation. H.323 at 27.

> RAS protocol is the registration and admission protocol implemented by the Gatekeeper:
>
> **7.2 Registration, Admission and Status (RAS) channel**
>
> The RAS Channel shall be used to carry messages used in the Gatekeeper discovery and endpoint registration processes which associate an endpoint's alias address with its Call Signaling Channel Transport Address. H.323 at 34.

Gatekeepers authenticate and encrypt RAS communications to/from endpoints to keep the secure name secure:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the ***RAS protocol***. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. ***Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.***
>
> 2. ***After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints.*** Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed. H.235 at 30-31.

In H.323, Alias names can be secure names and can provide access to the second device using a secure name service (i.e., the Gatekeeper computer):

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38.

As discussed above, networks that utilize Gateways also utilize Gatekeepers to translate, e.g., incoming E.164 addresses to Transport Addresses:

> Networks which contain Gateways should also contain a Gatekeeper in order to translate incoming E.164 or partyNumber addresses into Transport Addresses. H.323 at 28.

One example of the use of secure names and a secure name server in H.323 follows:

> This subclause will describe an example usage of security tokens to obscure or hide destination addressing information. The example scenario is an endpoint which wishes to make a call to another endpoint utilizing its well-known alias. More specifically, this involves an H.323 endpoint, gatekeeper, POTS-gateway, and telephone as illustrated below.

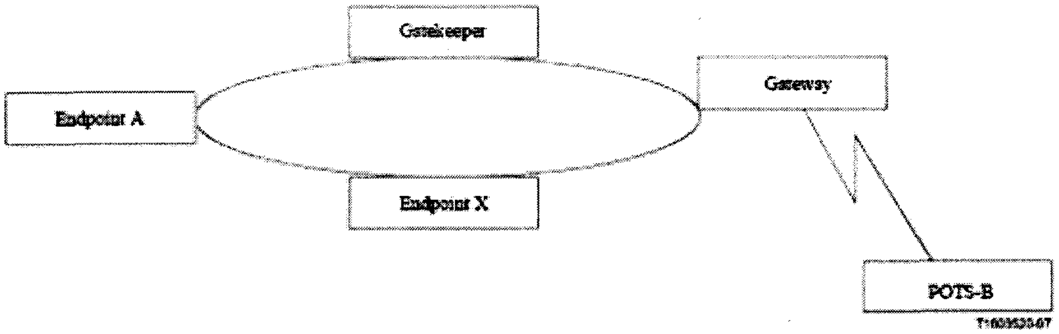


Figure I.6/H.235

> Assume that EPA [Endpoint A] is trying to call POTS-B, and POTS-B does not want to expose its E.164 phone number to EPA.
>
> - EPA will send an ARQ to its gatekeeper to resolve the address of the POTS telephone as represented by its alias/GW. The gatekeeper would recognize this as a "private" alias, knowing that in order to complete the connection it must return the POTS-gateway address (similar to returning the address of an H.320 gateway if an H.320 endpoint is called by an H.323 endpoint).
> - In the returned ACF, the gatekeeper returns the POTS-gateway's address as expected. The addressing information that is required to dial to the end telephone (i.e. the telephone number) is returned in an encrypted token included in the ACF. This encrypted token contains the actual E.164 (phone number) of the telephone which cannot be deciphered nor understood by the caller (i.e. EPA).
> - The endpoint issues the SETUP message to the gateway device (whose call signaling address was returned in the ACF) including the opaque token(s) that it received with the ACF.
> - The gateway, upon receiving the SETUP, issues its ARQ to its gatekeeper, including any token(s) that were received in the SETUP.
> - The gatekeeper is able to decipher the token(s) and return the phone number in the ACF. H.235 at 28-29

As indicated, in H.323, a first device sends a query to a secure name service (i.e., the Gatekeeper computer) requesting the network address associated with the secure name of a second device.

Alternatively, H.323 secures the name of an Alias address via IPSec when the calling endpoint queries the Gatekeeper:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application)

protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.

For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:

3. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. ***Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.***

4. ***After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints.*** Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed. H.235 at 30-31.

Step (b) of claim 2 further specifies: "at the first device, receiving a message containing the network address associated with the secure name of the second device; and"

As indicated in the example above, an address associated with the secure name is returned to the first device. For example, the address of the Gateway:

- EPA [Endpoint A] will send an ARQ to its gatekeeper to resolve the address of the POTS telephone as represented by its alias/GW. The gatekeeper would recognize this as a "private" alias, knowing that in order to complete the connection it must return the POTS-gateway address (similar to returning the address of an H.320 gateway if an H.320 endpoint is called by an H.323 endpoint).

- In the returned ACF, the gatekeeper returns the POTS-gateway's address as expected. The addressing information that is required to dial to the end telephone (i.e. the telephone number) is returned in an encrypted token included in the ACF. This encrypted token contains the actual E.164 (phone number) of the telephone which cannot be deciphered nor understood by the caller (i.e. EPA).

See H.235 at 28.

As indicated above, the Gatekeeper will know the endpoint associated with an Access token from the registration process and returns an IP address associated with the token so that calls can be routed through the Gatekeeper to the called endpoint:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> *See* H.323 at 38.

When an endpoint and a Gatekeeper use IPSec, the Gatekeeper returns the address to the calling endpoint in encrypted form:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. ***Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.***
>
> 2. ***After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact***

> ***this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints.*** Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> *See* H.235 at 30-31.

Step (c) of claim 2 further specifies: "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

The first device will send one or more messages to the network address associated with the secure name using a secure communication link, such as an IPSec connection or other secure link:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 3. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 4. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> 5. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 6. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by

> this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 7. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. Because the H.245 protocol is defined for the master to distribute the media keying material on the H.245 channel (to allow for multipoint communication), it is not recommended that IPSEC be used for the RTP channel.
>
> *See* H.235 at 30-31.

The first device may use call establishment security, call control security, and/or media stream privacy to communicate securely through a secure communication link:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.
>
> **6.4 Call control (H.245) security**
>
> The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.
>
> The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this. H.235 at 6.
>
> **6.5 Media stream privacy**

> This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.
>
> A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating endpoints may utilize an encrypted H.245 channel. In this manner, cryptographic algorithm selection and encryption keys as passed in the H.245 OpenLogicalChannel command are protected.
>
> The H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy. This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity.
>
> If it is required that the H.245 channel be operated in a non-encrypted manner, the specific media encryption keys may be encrypted separately in the manner signaled and agreed to by the participating parties. A logical channel of type h235Control may be utilized to provide the material to protect the media encryption keys. This logical channel may be operated in any appropriately negotiated mode.
>
> The privacy (encryption) of data carried in logical channels shall be in the form specified by the OpenLogicalChannel. Transport-specific header information shall not be encrypted. The privacy of data is to be based upon end-to-end encryption.
>
> *See* H.235 at 6-7.

Accordingly, H.323 anticipates claim 2 of the '181 patent under 35 U.S.C. § 102(b) above.

3. Claim 3

Claim 3 depends from claim 2, and specifies "wherein the secure name of the second device is a secure domain name.

During the prosecution of the '181 patent, the patent owners argued that a "secure name" can be a "secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a ***telephone number***." *See* Section III above. H.323 discloses that Alias names can be telephone numbers:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. *** These address[es] include E.164 or partyNumber addresses (network access number, telephone

> number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Thus, H.323 discloses a secure domain name under the construction provided by the Applicant.

Alternatively, because Alias names may take the form of H.323 IDs, any identifier could be used:

> The H.323 ID consists of a string of ISO/IEC 10646-1 characters as defined in Recommendation H.225.0. It may be a user name, conference name, e-mail name, or other identifier. H.323 at 34.

Accordingly, H.323 anticipates claim 3 of the '181 patent under 35 U.S.C. § 102(b) above.

4. Claim 4

Claim 4 depends from claim 2, and specifies "wherein the secure name indicates security."

The Gatekeeper recognizes the alias as a secure name:

- EPA will send an ARQ to its gatekeeper to resolve the address of the POTS telephone as represented by its alias/GW. The gatekeeper would ***recognize this as a "private" alias***, knowing that in order to complete the connection it must return the POTS-gateway address (similar to returning the address of an H.320 gateway if an H.320 endpoint is called by an H.323 endpoint). H.235 at 28.

Accordingly, H.323 anticipates claim 4 of the '181 patent under 35 U.S.C. § 102(b) above.

5. Claim 5

Claim 5 of the '181 patent depends from claim 2, and specifies "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form."

H.323 teaches use of IPSec for communications with the Gatekeeper, even when querying for a network address:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:

> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. ***Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint***. H.235 at 30.

Accordingly, H.323 anticipates claim 5 of the '181 patent under 35 U.S.C. § 102(b) above.

6. Claim 6

Claim 6 depends from claim 5, and specifies that the step of "further including decrypting the message."

As indicated above, the Gatekeeper encrypts the address and port number of the called endpoint and returns it to the calling endpoint. The calling endpoint would necessarily decrypt the message:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. ***Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.***
>
> 2. ***After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints.*** Upon completion of this negotiation, an IPSEC Security Association (SA) for

> the address/port will exist and the Q.931 signaling can proceed. H.235 at 30-31.

Accordingly, H.323 anticipates claim 6 of the '181 patent under 35 U.S.C. § 102(b) above.

7. Claim 7

Claim 7 of the '181 patent depends from claim 2, and specifies "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed."

H.323 device can communicate in the negotiated secure mode or unsecure mode:

> As stated in the system introduction clause, both the call connection channel (H.225.0 for H.323 series) and call control (H.245) channel shall operate in the negotiated secured or unsecured mode starting with the first exchange. H.235 at 8.

Accordingly, H.323 anticipates claim 7 of the '181 patent under 35 U.S.C. § 102(b) above.

8. Claim 8

Claim 8 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

The Transport address returned in the various embodiment discussed above can be IP addresses:

> **3.42 transport address**: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the ***Network Address*** plus the TSAP identifier [port number] of the addressable H.323 entity.
>
> **3.33 network address**: The network layer address of an H.323 entity as defined by the (inter)network layer protocol in use (e.g. an IP address). This address is mapped onto the layer one address of the respective system by some means defined in the (inter)networking protocol. H.323 at 7-8.

Accordingly, H.323 anticipates claim 8 of the '181 patent under 35 U.S.C. § 102(b) above.

9. Claim 9

Claim 9 depends from claim 2 and specifies that "further including automatically initiating the secure communication link after it is enabled."

The IPSec, TLS, and other communication links identified in claim 2 are initiated automatically.

Accordingly, H.323 anticipates claim 9 of the '181 patent under 35 U.S.C. § 102(b) above.

10. Claim 10

Claim 10 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.."

H.323 utilizes IPSec to secure the RAS channel for queries to the Gatekeeper:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. ***Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.***
>
> 2. ***After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints.*** Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> *See* H.235 at 30-31.

Accordingly, H.323 anticipates claim 10 of the '181 patent under 35 U.S.C. § 102(b) above.

11. Claim 11

Claim 11 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

The IPsec tunnel identified above would return the message containing the network address associated with the secure name in the form of at least one tunneled packet.

Accordingly, H.323 anticipates claim 11 of the '181 patent under 35 U.S.C. § 102(b) above.

12. Claim 12

Claim 12 depends from claim 2 and specifies "wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols."

H.323 endpoints use a variety of protocols, include TCP/IP, RTP, RCTP, IPSec, and each of the ITU-T Recommendations identified herein. For example, see the following:

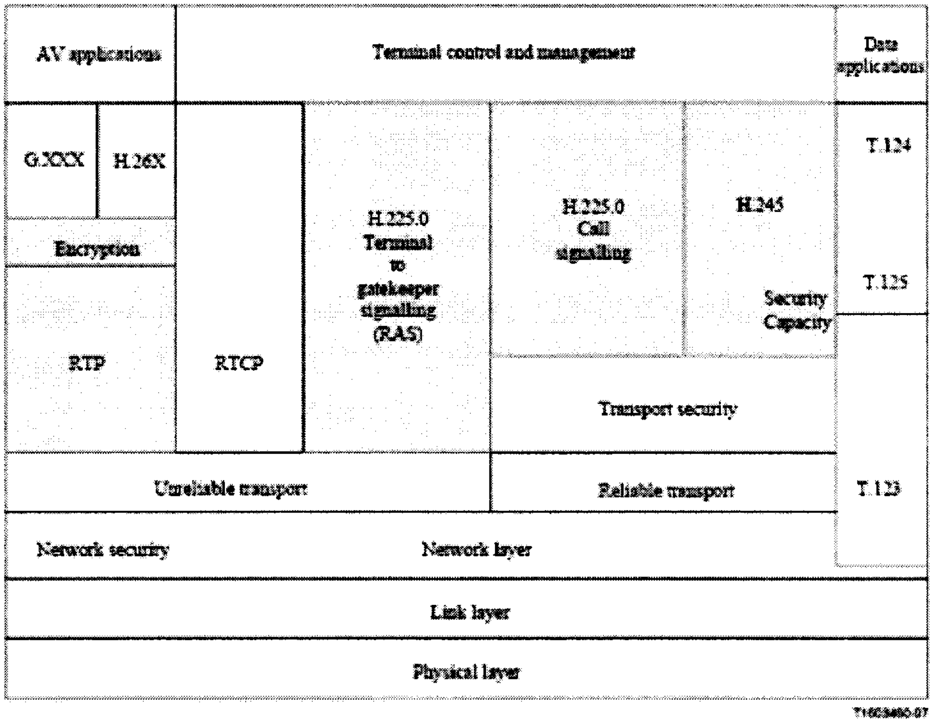


Figure B.1/H.235

H.235 at 20.

See also the following:

6.2.3 Packet based network interface

The packet based network interface is implementation-specific and is outside the scope of this Recommendation. However, the network interface shall provide the services described in Recommendation H.225.0. This includes the following: Reliable (e.g. TCP, SPX) end-to-end service is mandatory for the H.245 Control Channel, the Data Channels, and the Call Signaling Channel. Unreliable (e.g. UDP, IPX) end-to-end service is mandatory for the Audio Channels, the Video Channels, and the RAS Channel. These services may be duplex or simplex, unicast or multicast depending on the application, the capabilities of the terminals, and the configuration of the network. H.323 at 14.

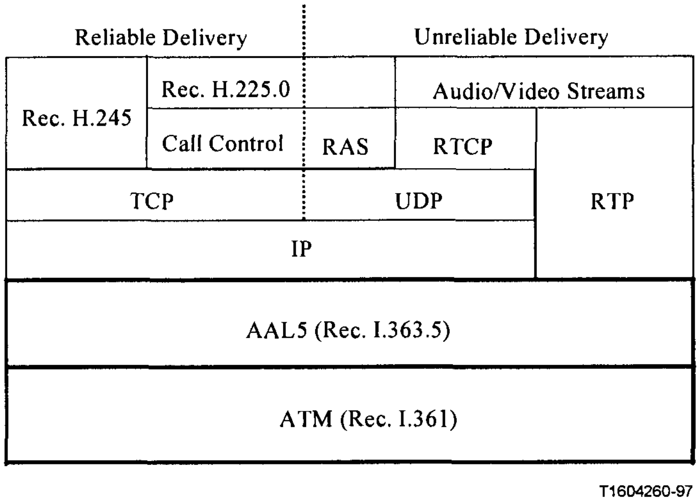


Figure C.1/H.323 – Architecture for H.323 on ATM-AAL5

H.323 at 96.

Accordingly, H.323 anticipates claim 12 of the '181 patent under 35 U.S.C. § 102(b) above.

13. Claim 13

Claim 13 depends from claim 2 and specifies "wherein the receiving and sending of messages through the secure communication link includes multiple sessions."

H.323 teaches that multiple RTP channels or sessions are sent and/or received through the secure communication link:

B.6.1 Multiple logical channels and RTP sessions for a layered stream

> If bandwidth scaling is the goal of using layering, each layer should flow on a separate logical channel with a separate RTP session. This means that what is a single video source will now have to be coordinated amongst multiple logical channels and RTP sessions. H.323 at 91.

See also the following:

> For efficient protocol processing, the number of multiplexing points should be minimized, as described in the integrated layer processing design principle [A-1]. In RTP, multiplexing is provided by the destination transport address (network address and port number) which define an RTP session. For example, in a teleconference composed of audio and video media encoded separately, each medium should be carried in a separate RTP session with its own destination transport address. It is not intended that the audio and video be carried in a single RTP session and demultiplexed based on the payload type or SSRC fields. H.225 at 73.

Accordingly, H.323 anticipates claim 13 of the '181 patent under 35 U.S.C. § 102(b) above.

14. Claim 14

Claim 14 depends from claim 2 and specifies "further including supporting a plurality of services over the secure communication link."

The secure communication links identified above support multiple services. For example, see the following:

> **6.2.3 Packet based network interface**
>
> The packet based network interface is implementation-specific and is outside the scope of this Recommendation. However, the network interface shall provide the services described in Recommendation H.225.0. This includes the following: Reliable (e.g. TCP, SPX) end-to-end service is mandatory for the H.245 Control Channel, the Data Channels, and the Call Signaling Channel. Unreliable (e.g. UDP, IPX) end-to-end service is mandatory for the Audio Channels, the Video Channels, and the RAS Channel. These services may be duplex or simplex, unicast or multicast depending on the application, the capabilities of the terminals, and the configuration of the network. H.323 at 14.
>
> All call signaling received by the Gateway from an SCN endpoint and not applicable to the Gateway should be passed through to the network endpoint, and vice versa. This signaling includes, but is not limited to, Q.932, Q.950, and H.450-Series messages. This will allow H.323 endpoints to implement the Supplementary Services defined in those Recommendations. H.323 at 25.
>
> This Recommendation provides a number of different services, some of which are expected to be applicable to all terminals that use it and some that are more specific to particular ones. Procedures are defined to allow the exchange of audiovisual and data capabilities, to request the transmission of a particular audiovisual and data mode, to

> manage the logical channels used to transport the audiovisual and data information, to establish which terminal is the master terminal and which is the slave terminal for the purposes of managing logical channels, to carry various control and indication signals, to control the bit rate of individual logical channels and the whole multiplex, and to measure the round trip delay, from one terminal to the other and back. H.225 at 73.

Accordingly, H.323 anticipates claim 14 of the '181 patent under 35 U.S.C. § 102(b) above.

15. Claim 15

Claim 15 depends from claim 14 and specifies "wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof."

As indicated above for claims 12-14, the plurality of services includes a plurality of communication protocols, multiple sessions, application programs, or a combination thereof.

Accordingly, H.323 anticipates claim 15 of the '181 patent under 35 U.S.C. § 102(b) above.

16. Claim 16

Claim 16 depends from claim 15 and specifies that "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof."

H.323 teaches use of multimedia services, including video conferencing and telephony:

> H.323 entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork. H.323 at (i).
>
> H.323 entities may be integrated into personal computers or implemented in stand-alone devices such as videotelephones. H.323 at (i). Data signals include still pictures, facsimile, documents, computer files and other data streams. H.323 at 13.

Facsimile is an example of telephony services. For additional telephony services, see, e.g., H.323 at 79, and the following

> **3.7 call**: Point-to-point multimedia communication between two H.323 endpoints. The call begins with the call set-up procedure and ends with the call termination procedure. The call consists of the collection of reliable and unreliable channels between the endpoints. A call may be directly between two endpoints, or may include other H.323 entities such as a Gatekeeper or MC. In case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway where they are converted to the appropriate representation for the SCN end system. Typically, a call is between two users

> for the purpose of communication, but may include signaling-only calls. An endpoint may be capable of supporting multiple simultaneous calls. H.323 at 4-5.

Accordingly, H.323 anticipates claim 16 of the '181 patent under 35 U.S.C. § 102(b) above.

17. Claim 17

Claim 17 depends from claim 15 and specifies that "wherein the plurality of services comprises audio, video or a combination thereof.."

H.323 teaches use of multimedia services, including video conferencing and telephony:

> H.323 entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork. H.323 at (i).
>
> H.323 entities may be integrated into personal computers or implemented in stand-alone devices such as videotelephones. H.323 at (i).Data signals include still pictures, facsimile, documents, computer files and other data streams. H.323 at 13.

Facsimile is an example of telephony services. For additional telephony services, see, e.g., H.323 at 79, and the following

> **3.7 call**: Point-to-point multimedia communication between two H.323 endpoints. The call begins with the call set-up procedure and ends with the call termination procedure. The call consists of the collection of reliable and unreliable channels between the endpoints. A call may be directly between two endpoints, or may include other H.323 entities such as a Gatekeeper or MC. In case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway where they are converted to the appropriate representation for the SCN end system. Typically, a call is between two users for the purpose of communication, but may include signaling-only calls. An endpoint may be capable of supporting multiple simultaneous calls. H.323 at 4-5.

Accordingly, H.323 anticipates claim 17 of the '181 patent under 35 U.S.C. § 102(b) above.

18. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

H.323 teaches that the communication links identified above are authenticated links:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application)

protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.

For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:

1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.

2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.

3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.

4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.

5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. Because the H.245 protocol is defined for the master to distribute the media keying material on the H.245 channel (to allow for multipoint communication), it is not recommended that IPSEC be used for the RTP channel. H.235 at 30-31.

Accordingly, H.323 anticipates claim 18 of the '181 patent under 35 U.S.C. § 102(b) above.

19. Claim 19

Claim 19 depends from claim 2 and specifies "wherein the first device is a computer, and the steps are performed on the computer."

H.323 entities include computers:

> H.323 entities may be integrated into personal computers or implemented in stand-alone devices such as videotelephones. H.323 at (i).

Accordingly, H.323 anticipates claim 19 of the '181 patent under 35 U.S.C. § 102(b) above.

20. Claim 20

Claim 20 depends from claim 2 and specifies "wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network."

H.323 entities include client computers where the method steps performed above for the first device can be performed by the client computer:

> H.323 entities may be integrated into personal computers or implemented in stand-alone devices such as videotelephones. H.323 at (i).

Accordingly, H.323 anticipates claim 20 of the '181 patent under 35 U.S.C. § 102(b) above.

21. Claim 21

Claim 21 depends from claim 2 and specifies "further including providing an unsecured name associated with the device."

H.323 teaches providing an unsecured name associated with the device. For example, H.323 teaches endpoints can register more than one Alias address with a Gatekeeper:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and ***alias addresses***. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint powerup). H.323 at 35.

From the teachings of H.323, one could register an unsecured name and a secure name for a single device. For example, a single endpoint may have multiple aliases, including an alias that represents the endpoint and an alias that may represent conferences the endpoint hosts, as indicated above.

Alternatively, endpoints can register a secure name and be associated with the unsecured name of the Gatekeeper computer with which they are registered. For example, endpoints issue a Registration Request (RRQ) to a Gatekeeper to register their aliases and the Gatekeeper responds with a Registration Confirmation (RCF):

> An endpoint shall send a Registration Request (RRQ) to a Gatekeeper. This is sent to the Gatekeeper's RAS Channel Transport Address. The endpoint has the Network Address of the Gatekeeper from the Gatekeeper discovery process and uses the well-known RAS Channel TSAP Identifier. The Gatekeeper shall respond with either a Registration Confirmation (RCF) or a Registration Reject (RRJ). H.323 at 35

Gatekeepers have unsecured names registered in the public DNS:

> **IV.1.1.2 Discovery using DNS (informative)**
>
> **IV.1.1.2.1 A URL for gatekeepers**
>
> As a first step, note that a gatekeeper is identified by a transport address and a gatekeeperIdentifier, which is a string. A gatekeeper is a particular resource on the Internet, so it is reasonable to specify it in a Uniform Resource Locator (URL). The protocol spoken by the gatekeeper is RAS, so the URL for a gatekeeper could be given by:
>
> ras://gkID@domainname
>
> gkID is the gatekeeperIdentifier, and domainname is a DNS domain name which identifies the gatekeeper's domain. Note that this is not necessarily a Fully Qualified Domain Name (FQDN) with an A-record – it is not required that this domain name has a physical transport interface with an IP number recorded in the DNS. If it is a FQDN, however, it is reasonable to insist that its IP number is that of the gatekeeper to which the URL refers. In this case, it is allowed to add an optional port number to the URL:
>
> ras://gkID@domainname:port_no.
>
> If no port number is given, then the well known value of 1719 is taken as a default.

> The more interesting case is when this is not an FQDN, and then the domain name does not refer to a transport address listed in the DNS. The domain name then can refer to a pure "gatekeeper zone of authority". The next subclause explains how to find the gatekeeper in this case.
>
> *See* H.225 at 141.

See also, H.225 at 141-143, describing use of the DNS TXT and DNS SRV Resource Records in the public, Internet domain name system for locating the proper Gatekeeper computer on which a particular H.323 terminal is registered. The name corresponding to Gatekeeper computer for the H.323 endpoint is an unsecured name associated with the endpoint.

In other words, each endpoint can register a secure name with its Gatekeeper and be located on the Internet using the domain name associated with the endpoint in the public DNS, which identifies the endpoint's Gatekeeper computer.

Alternatively, MCUs and Gateways are endpoints and register multiple Alias names, as well:

> **3.14 endpoint**: An H.323 terminal, ***Gateway***, or MCU. An endpoint can call and be called. It generates and/or terminates information streams. H.323 at 5.
>
> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. H.323 at 33.

A Gateway is an endpoint on a packet-based network that connects the packet-based network to a circuit-switched network where other ITU Terminals (endpoints) reside, or to another H.323 Gateway:

> **3.16 gateway**: An H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 Terminals on the packet based network and other ITU Terminals on a switched circuit network, or to another H.323 Gateway. Other ITU Terminals include those complying with Recommendations H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.324 (GSTN), H.324M (Mobile), and V.70 (DSVD). H.323 at 5.

Gateways and MCUs may register two or more Transport Addresses for each Alias address:

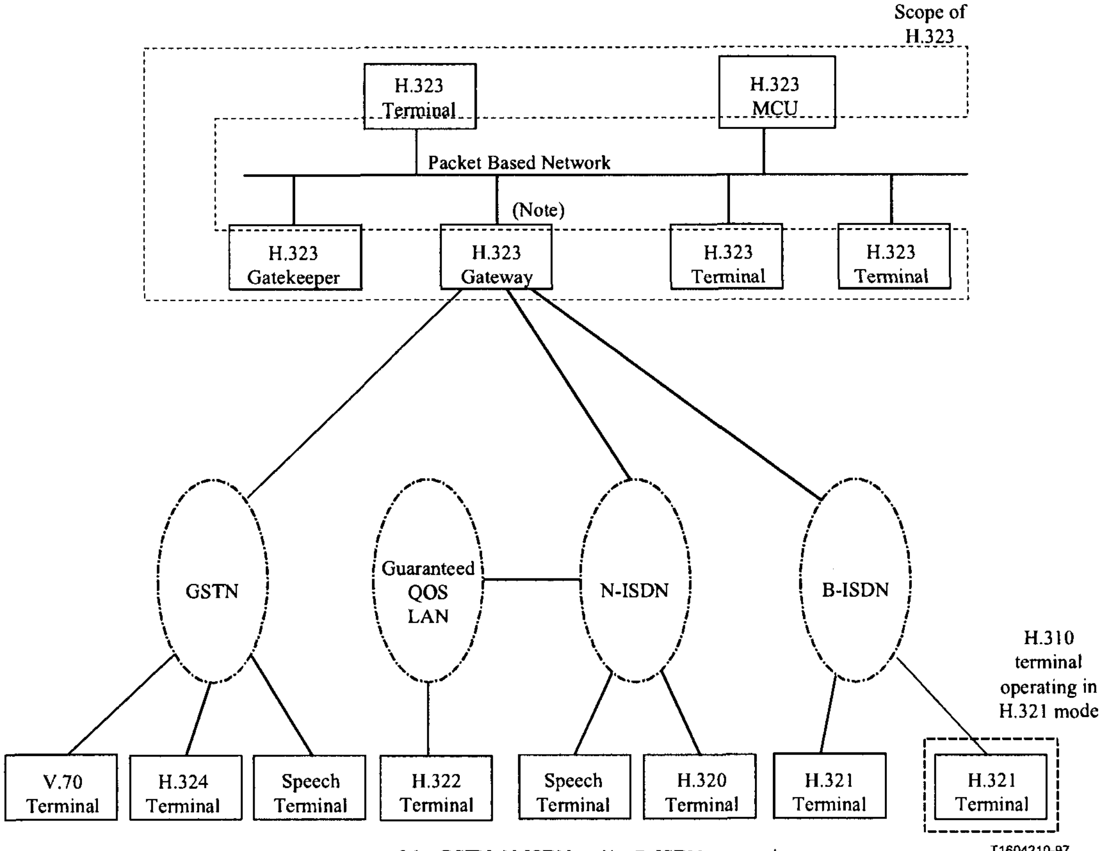
> A Gateway or MCU may register a single Transport Address or multiple Transport Addresses. The use of multiple Transport Addresses may simplify the routing of calls to specific ports. H.323 at 35.

A single Gateway may terminate calls to multiple Switched Circuit Network (SCN) endpoints:

> **3.7 call**: Point-to-point multimedia communication between two H.323 endpoints. The call begins with the call set-up procedure and ends with the call termination procedure. The call consists of the collection of reliable and unreliable channels between the

> endpoints. A call may be directly between two endpoints, or may include other H.323 entities such as a Gatekeeper or MC. ***In case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway*** where they are converted to the appropriate representation for the SCN end system. Typically, a call is between two users for the purpose of communication, but may include signaling-only calls. An endpoint may be capable of supporting multiple simultaneous calls. H.323 at 5-6.

See also, Figure 1 below (H.323 at 2) showing an H.323 Gateway connecting multiple SCN devices to the packet-based network via different switched circuit networks (SCNs):



NOTE – A gateway may support one or more of the GSTN, N-ISDN and/or B-ISDN connections.

As indicated SCN means "Switched Circuit Network" and includes GSTN, N-ISDN, and B-ISDN networks:

> **3.40 Switched Circuit Network (SCN)**: A public or private switched telecommunications network such as the GSTN, N-ISDN, or B-ISDN.
>
> NOTE – While B-ISDN is not strictly a switched circuit network, it exhibits some of the characteristics of an SCN through the use of virtual circuits.

Thus, each H.323 endpoint is associated with both a secure name (i.e., Access Token) and an unsecured name (i.e., either another Alias name, the name in the DNS system for locating the Gatekeeper computer in which it is registered, or for a Gateway endpoint, two devices obtaining access to the packet-based network through the Gateway, one having a secure name and the other an unsecured name).

Accordingly, H.323 anticipates claim 21 of the '181 patent under 35 U.S.C. § 102(b) above.

22. Claim 22

Claim 22 depends from claim 2 and specifies "wherein the secure name is registered prior to the step of sending a message to a secure name service."

H.323 teaches that the secure name is registered prior to the set of sending a message to a secure name service:

> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. ***Registration shall occur before any calls are attempted and may occur periodically as necessary*** (for example, at endpoint powerup).
>
> *See* H.323 at 35 (emphasis added).

Accordingly, H.323 anticipates claim 22 of the '181 patent under 35 U.S.C. § 102(b) above.

23. Claim 23

Claim 23 depends from claim 2 and specifies "wherein the secure name of the second device is a secure, non-standard domain name."

During the prosecution of the '181 patent, the patent owners argued that a "secure name" can be a "secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a ***telephone number***." *See* Section III above, for example.

H.323 discloses that Alias names can be telephone numbers:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. *** These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Thus, H.323 discloses a secure domain name under the construction provided by the Applicant.

Alternatively, because Alias names may take the form of H.323 IDs, any identifier could be used:

> The H.323 ID consists of a string of ISO/IEC 10646-1 characters as defined in Recommendation H.225.0. It may be a user name, conference name, e-mail name, or other identifier. H.323 at 34.

Accordingly, H.323 anticipates claim 23 of the '181 patent under 35 U.S.C. § 102(b) above.

24. Claim 24

Independent claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network, the method comprising:

> (a) at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;
>
> (b) receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and
>
> (c) sending a message securely from the first device to the second device."

The H.323 Recommendation discloses "[a] method of using a first device to securely communicate with a second device over a communication network" because it details secure, multimedia communications between two devices over a packet-based network, such as the Internet:

> This Recommendation covers the technical requirements for multimedia communications systems in those situations where the underlying transport is a Packet Based Network (PBN) .... These packet-based networks may include Local Area Networks, Enterprise Area Networks, Metropolitan Area Networks, Intra-Networks, and Inter- Networks (including the Internet). H.323 at 1.

Step (a) of claim 24 further specifies: "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

The H.323 recommendation discloses a system whereby each communicating device on a network can request and obtain registration of a secure name for the device, called an "Alias Address," which is associated with a network address. The Alias address can, for example, be an email address or an alphanumeric string in the form of an email address:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number,

> telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Alias Addresses can be "secure names" because, among other reasons, they can be protected by "access tokens," which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38.

Alias addresses are resolved into network addresses, such as IP addresses, by a Gatekeeper computer. The Gatekeeper provides a number of services, including address translation:

> Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed. H.323 at 27.

Transport Addresses are IP addresses in packet-based networks utilizing TCP/IP:

> **3.42 transport address**: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the ***Network Address*** plus the TSAP identifier [port number] of the addressable H.323 entity.
>
> **3.33 network address**: The network layer address of an H.323 entity as defined by the (inter)network layer protocol in use (e.g. an IP address). This address is mapped onto the layer one address of the respective system by some means defined in the (inter)networking protocol. H.323 at 7-8.

The endpoints of the H.323 recommendation, i.e., the devices desiring to securely communicate, must register their Alias and transport addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Further, endpoints may register "one or more alias addresses associated with it." *See, e.g.*, H.323 at 33.

Step (b) of claim 24 further specifies: "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and."

H.323 expressly references the authentication and security services that are described in H.235. Although "authentication and security for H.323 systems is optional," if it is provided, "it shall be provided in accordance with Recommendation H.235." H.323 at 81.

The Access tokens have two uses in the H.323 recommendation: to shield an endpoint's alias name and transport address, when desired, and to ensure that a calling endpoint can access the called endpoint directly:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 in 38.

As described in H.235, IPSec can then be used to secure communications between the two endpoints:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> 3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. H.235 at 30-31.

See also, H.235 at 6, which describes call establishment security call control security, and media stream privacy, in which all communications are secure.

Step (c) of claim 24 further specifies: "sending a message securely from the first device to the second device.

The H.235 protocol of the H.323 recommendation describes call establishment security, call control security, and media stream privacy, in which all communications are sent securely. H.235 at 6. For example:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.
>
> **6.4 Call control (H.245) security**
>
> The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.
>
> The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this.
>
> **6.5 Media stream privacy**
>
> This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

> A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. H.235 at 6.

Accordingly, the H.323 Recommendation anticipates claim 24 of the '181 patent under 35 U.S.C. § 102(b).

25. Claim 25

Claim 25 depends from claim 24 and specifies "wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link."

The endpoints of the H.323 recommendation, i.e., the devices desiring to communicate, register their alias address and transport addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Further, Alias Addresses can be secure names:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. ***The Gatekeeper will know the endpoint related to the Access Token from the registration process***, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. ***An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint***. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers. H.323 at 38 (emphasis added).

Accordingly, the H.323 recommendation anticipates claim 25 of the '181 patent under 35 U.S.C. § 102(b).

26. Claim 26

Independent claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising:

> (a) from the first device requesting and obtaining registration of an unsecured name associated with the first device;
>
> (b) from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;
>
> (c) receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and
>
> (d) from the first device sending a message securely from the first device to the second device."

The H.323 Recommendation discloses "[a] method of using a first device to securely communicate with a second device over a communication network" because it details secure, multimedia communications between two devices over a packet-based network, such as the Internet:

> This Recommendation covers the technical requirements for multimedia communications systems in those situations where the underlying transport is a Packet Based Network (PBN) .... These packet-based networks may include Local Area Networks, Enterprise Area Networks, Metropolitan Area Networks, Intra-Networks, and Inter- Networks (including the Internet). H.323 at 1.

Step (a) of claim 26 further specifies: "from the first device requesting and obtaining registration of an unsecured name associated with the first device"

As described in the H.323 recommendation, each communicating device (i.e., endpoint) on a network can request and obtain registration of an unsecured name for the device, called an Alias Address, which is associated with a network address. The Alias address can, e.g., be an email address or an alphanumeric string in the form of an email address:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number,

> telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0. H.323 at 33-34.

Endpoints register their Alias Address and Transport Addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up). H.323 at 35.

Endpoints may register more than one alias address, H.323 at 33, and alias addresses can be, but does not necessarily have to be, secure names:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers.
>
> *See* H.323 at 38.

Step (b) of claim 26 further specifies: "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device"

As indicated above, each communicating device on a network can request and obtain registration of a secure name for the device, called an Alias Address, which is associated with a network address. The Alias address can, e.g., be an email address or an alphanumeric string in the form of an email address:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting. The alias addresses provide an alternate method of addressing the endpoint. These address[es] include E.164 or partyNumber addresses (network access number, telephone number, etc.), H.323 IDs (alphanumeric strings representing names, e-mail like addresses, etc.), and any others defined in Recommendation H.225.0.
>
> *See* H.323 at 33-34.

Endpoints register their Alias Address and Transport Addresses with the Gatekeeper:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up).
>
> *See* H.323 at 35.

In the H.323 recommendation, "Alias Address" can constitute "secure names" because, for example, they can be protected by "access tokens," which have the function of ensuring the anonymity of an endpoint's Transport Address and Alia Address:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers.
>
> *See* H.323 at 38.

As indicated above, endpoint registration includes registering multiple transport and alias addresses:

> **7.9.1 RegistrationRequest (RRQ)**
>
> The RRQ message includes the following:
>
> ***
>
> **callSignalAddress** – This is the call signaling transport address for this endpoint. If multiple transports are supported, they must be registered all at once.
>
> ***
>
> **terminalAlias** -This optional value is a list of alias addresses, by which other terminals may identify this terminal. If the terminalAlias is null, or an E.164 address is not present, an E.164 address may be assigned by the gatekeeper, and included in the RCF. If an email-ID is available for the endpoint, it should be registered. Note that multiple alias addresses may refer to the same transport addresses. All of the endpoint's aliases shall be included in each RRQ.
>
> *See* H.225.0 at 45.

From the teachings of H.323, one could register an unsecured name and a secure name for a single device. For example, a single endpoint may have multiple aliases, including an alias that represents the endpoint and an alias that represents conferences the endpoint hosts:

> **7.1.3 Alias address**
>
> An endpoint may also have one or more alias addresses associated with it. An alias address may represent the endpoint or it may represent conferences that the endpoint is hosting.
>
> *See* H.323 at 33.

In this manner, an endpoint device following the H.323 recommendation would have had the capability of registering both a secure and an unsecure name. Moreover, MCUs and Gateways are endpoints:

> **3.14 endpoint**: An H.323 terminal, Gateway, or MCU. An endpoint can call and be called. It generates and/or terminates information streams. H.323 at 5.

A Gateway is an endpoint on a packet-based network that connects the packet-based network to a circuit-switched network where other ITU Terminals (endpoints) reside, or to another H.323 Gateway:

> **3.16 gateway**: An H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 Terminals on the packet based

> network and other ITU Terminals on a switched circuit network, or to another H.323 Gateway. Other ITU Terminals include those complying with Recommendations H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.324 (GSTN), H.324M (Mobile), and V.70 (DSVD). H.323 at 5.

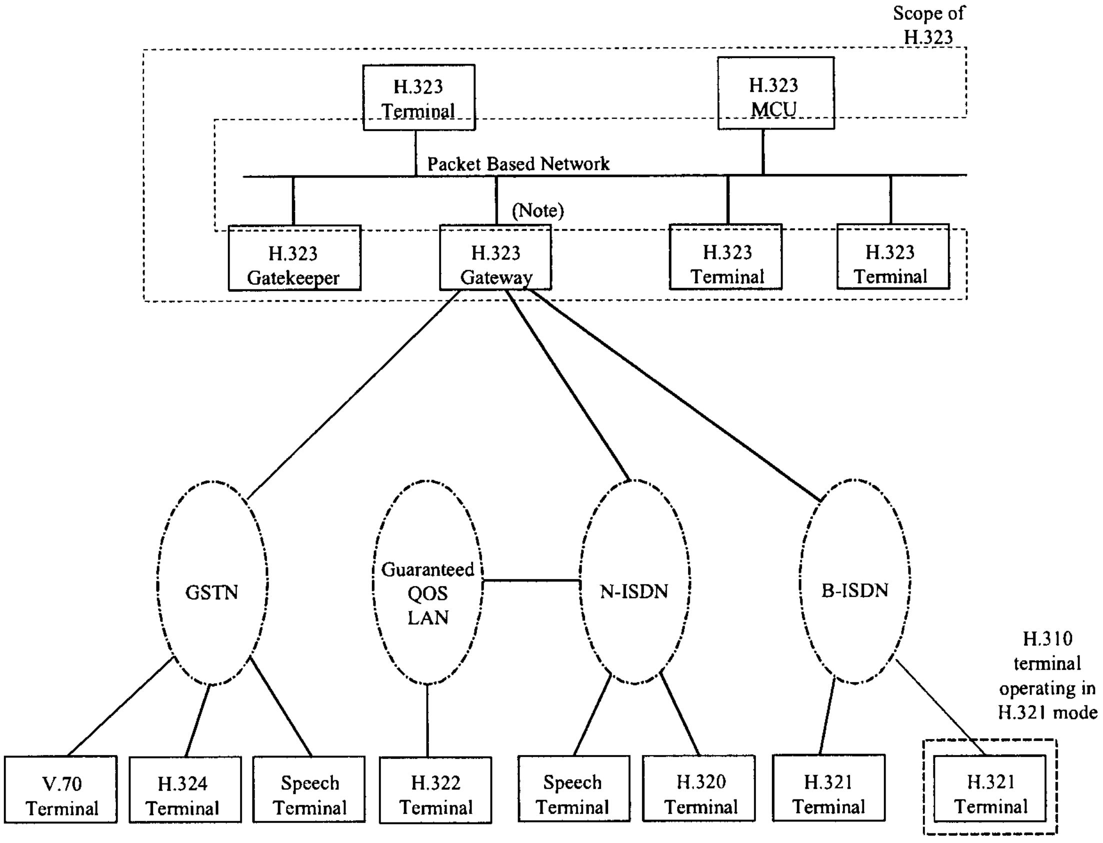
Gateways and MCUs may register two or more Transport Addresses:

> A Gateway or MCU may register a single Transport Address or multiple Transport Addresses. The use of multiple Transport Addresses may simplify the routing of calls to specific ports. H.323 at 35.

A single Gateway may terminate calls to multiple Switched Circuit Network (SCN) endpoints:

> **3.7 call**: Point-to-point multimedia communication between two H.323 endpoints. The call begins with the call set-up procedure and ends with the call termination procedure. The call consists of the collection of reliable and unreliable channels between the endpoints. A call may be directly between two endpoints, or may include other H.323 entities such as a Gatekeeper or MC. ***In case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway*** where they are converted to the appropriate representation for the SCN end system. Typically, a call is between two users for the purpose of communication, but may include signaling-only calls. An endpoint may be capable of supporting multiple simultaneous calls.
>
> *See* H.323 at 5-6.

See also, Figure 1 below (H.323 at 2) showing an H.323 Gateway connecting multiple SCN devices to the packet-based network via different switched circuit networks (SCNs):



NOTE – A gateway may support one or more of the GSTN, N-ISDN and/or B-ISDN connections.

As indicated SCN means "Switched Circuit Network" and includes GSTN, N-ISDN, and B-ISDN networks:

> **3.40 Switched Circuit Network (SCN)**: A public or private switched telecommunications network such as the GSTN, N-ISDN, or B-ISDN.
>
> NOTE – While B-ISDN is not strictly a switched circuit network, it exhibits some of the characteristics of an SCN through the use of virtual circuits.
>
> A Gateway or MCU may register a single Transport Address or multiple Transport Addresses. The use of multiple Transport Addresses may simplify the routing of calls to specific ports. H.323 at 35.

Step (c) of claim 26 further specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and"

H.323 expressly references the authentication and security services that are described in H.235. Although "authentication and security for H.323 systems is optional," if it is provided, "it shall be provided in accordance with Recommendation H.235." H.323 at 81.

The Access tokens have two uses in the H.323 recommendation: to shield an endpoint's alias name and transport address, when desired, and to ensure that a calling endpoint can access the called endpoint directly:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. The Gatekeeper will know the endpoint related to the Access Token from the registration process, so that calls using the Access Token can be routed through the Gatekeeper to the called endpoint. The use of the access token only applies to the Gatekeeper routed call model when attempting to hide the transport address from the endpoint.
>
> The second use of the Access Token is in ensuring that calls are routed properly through H.323 entities. An Access Token returned by a Gatekeeper shall be used in any subsequent setup messages sent by the endpoint. This Access Token may be used by a Gateway to assure that the endpoint has permission to use the Gateway resources, or it may be used by a called endpoint to assure that the calling endpoint can signal it directly.
>
> The Access Token may also be distributed by out-of-band methods to assure proper access to Gateways and endpoints in systems which do not have Gatekeepers.
>
> *See* H.323 in 38.

As described in H.235, IPSec can then be used to secure communications between the two endpoints:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 6. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.

> 7. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> 8. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 9. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 10. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel.
>
> *See* H.235 at 30-31.

See also, H.235 at 6, which describes call establishment security call control security, and media stream privacy, in which all communications are secure.

Step (d) of claim 26 further specifies: "from the first device sending a message securely from the first device to the second device."

The H.235 protocol of the H.323 recommendation describes call establishment security, call control security, and media stream privacy, in which all communications are sent securely. H.235 at 6. For example:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.

6.4 Call control (H.245) security

The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.

The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this.

6.5 Media stream privacy

This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams.

See H.235 at 6.

Accordingly, the H.323 recommendation anticipates claim 26 under 35 U.S.C. § 102(b).

27. Claim 27

Claim 27 depends from claim 26 and specifies:

(a) "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

(b) wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

Step (a) of claim 27 specifies: "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

As indicated above, all H.323 endpoints register their aliases:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up).
>
> H.323 at 35.

Step (b) of claim 27 specifies: wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

As indicated above, all H.323 endpoints register their aliases:

> **7.2.2 Endpoint registration**
>
> Registration is the process by which an endpoint joins a Zone, and informs the Gatekeeper of its Transport Address and alias addresses. As part of their configuration process, all endpoints shall register with the Gatekeeper identified through the discovery process. Registration shall occur before any calls are attempted and may occur periodically as necessary (for example, at endpoint power- up).
>
> *See* H.323 at 35.

Endpoints register their Access Tokens for secure names:

> **7.2.5 Access tokens**
>
> An Access Token is a string passed in some RAS messages and the Setup message. The Access Tokens have two uses. First, they can provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party. A user may give out only the Access Token for a calling party to use in reaching the endpoint. ***The Gatekeeper will know the endpoint related to the Access Token from the registration process****....*
>
> *See* H.323 at 38.

Accordingly, H.323 anticipates claim 27 of the '181 patent under 35 U.S.C. § 102(b) above.

28. Claim 28

Independent claim 28 is directed to "[a] non-transitory machine-readable medium comprising instructions for:

(a) sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

(b) receiving a message containing the network address associated with the secure name of the device; and

(c) sending a message to the network address associated with the secure name of the device using a secure communication link.

The preamble of claim 28 specifies "[a] non-transitory machine-readable medium comprising instructions ...." Each device in H.323 network will include a non-transitory machine readable (e.g., a storage device) which is comprises executable code (e.g., "instructions") that enable the device to communicate with a first associated with a secure name. *See* H.323 at 1-2.

Step (a) of Claim 28 specifies: "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device."

In H.323, Gatekeepers are a secure name service. For example, Gatekeepers perform network address translation and admission control, i.e., authorize access to the network for the endpoints in the Gatekeepers Zone:

> When it is present in a system, the Gatekeeper shall provide the following services:
>
> - Address Translation – The Gatekeeper shall perform alias address to Transport Address translation. This should be done using a translation table which is updated using the Registration messages described in clause 7. Other methods of updating the translation table are also allowed.
>
> - Admissions Control – The Gatekeeper shall authorize network access using ARQ/ACF/ARJ H.225.0 messages. This may be based on call authorization, bandwidth, or some other criteria which is left to the manufacturer. It may also be a null function which admits all requests.
>
> - Zone Management – The Gatekeeper shall provide the above functions for terminals, MCUs, and Gateways which have registered with it as described in 7.2. H.323 at 27.
>
> **3.49 zone**: A Zone (see Figure 3) is the collection of all terminals (Tx), Gateways (GW), and Multipoint Control Units (MCUs) managed by a single Gatekeeper (GK). A Zone includes at least one terminal, and may or may not include Gateways or MCUs. A Zone has one and only one Gatekeeper. A Zone may be independent of network topology and

> may be comprised of multiple network segments which are connected using routes (R) or other devices.
>
> *See* H.323 at 8.

Gatekeepers implement call authorization, restricting access to certain terminals or gateways:

> Call Authorization – Through the use of the H.225.0 signaling, the Gatekeeper may reject calls from a terminal due to authorization failure. The reasons for rejection may include, but are not limited to, restricted access to/from particular terminals or Gateways, and restricted access during certain periods of time. The criteria for determining if authorization passes or fails is outside the scope of this Recommendation. H.323 at 27.
>
> RAS protocol is the registration and admission protocol implemented by the Gatekeeper:
>
> **7.2 Registration, Admission and Status (RAS) channel**
>
> The RAS Channel shall be used to carry messages used in the Gatekeeper discovery and endpoint registration processes which associate an endpoint's alias address with its Call Signaling Channel Transport Address.
>
> *See* H.323 at 34.

Gatekeepers authenticate and encrypt RAS communications sent to / received from endpoints to keep the secure name secure using, e.g., IPSec:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
> 2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair.

> Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.

Step (b) of claim 28 specifies: "receiving a message containing the network address associated with the secure name of the device"

Endpoints receive the network address returned from the Gatekeeper:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 2. ***After obtaining the address and port number*** of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> *See* H.235 at 30.

Step (c) of claim 28 specifies: "sending a message to the network address associated with the secure name of the device using a secure communication link."

Endpoints contact the calling party and communicate securely:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application)

protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.

For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:

1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.

2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.

3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.

4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.

5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. Because the H.245 protocol is defined for the master to distribute the media keying material on the H.245 channel (to allow for multipoint communication), it is not recommended that IPSEC be used for the RTP channel.

See H.235 at 30-31.

Security includes call establishment security, call control security, and media stream privacy, all include sending a message to the network address associated with the secure name:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.
>
> **6.4 Call control (H.245) security**
>
> The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.
>
> The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this. H.235 at 6.
>
> **6.5 Media stream privacy**
>
> This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.
>
> A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating endpoints may utilize an encrypted H.245 channel. In this manner, cryptographic algorithm selection and encryption keys as passed in the H.245 OpenLogicalChannel command are protected.

> The H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy. This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity.
>
> If it is required that the H.245 channel be operated in a non-encrypted manner, the specific media encryption keys may be encrypted separately in the manner signaled and agreed to by the participating parties. A logical channel of type h235Control may be utilized to provide the material to protect the media encryption keys. This logical channel may be operated in any appropriately negotiated mode.
>
> The privacy (encryption) of data carried in logical channels shall be in the form specified by the OpenLogicalChannel. Transport-specific header information shall not be encrypted. The privacy of data is to be based upon end-to-end encryption. H.235 at 6-7.

Accordingly, H.323 anticipates claim 28 of the '181 patent under 35 U.S.C. § 102(b) above.

29. Claim 29

Independent claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

> (a) receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and
>
> (b) sending a message securely from the first device to the second device.

The preamble of claim 29 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name ...." Each device in H.323 network will include a non-transitory machine readable (e.g., a storage device) which is comprises executable code (e.g., "instructions") that enable the device to communicate with a first associated with a secure name. *See* H.323 at 1.

Step (a) of Claim 29 specifies: "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered"

H.323 teaches receiving at network address associated with a secure name a message from a second device requesting the desire to securely communicate:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.

> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.
>
> 3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. Because the H.245 protocol is defined for the master to distribute the media keying material on the H.245 channel (to allow for multipoint communication), it is not recommended that IPSEC be used for the RTP channel.
>
> *See* H.235 at 30-31.

Security includes call establishment security, call control security, and media stream privacy, all include sending a message to the network address associated with the secure name:

6.3 Call establishment security

There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.

6.4 Call control (H.245) security

The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.

The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this.

See H.235 at 6.

6.5 Media stream privacy

This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating endpoints may utilize an encrypted H.245 channel. In this manner, cryptographic algorithm selection and encryption keys as passed in the H.245 OpenLogicalChannel command are protected.

The H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy.

> This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity.
>
> If it is required that the H.245 channel be operated in a non-encrypted manner, the specific media encryption keys may be encrypted separately in the manner signaled and agreed to by the participating parties. A logical channel of type h235Control may be utilized to provide the material to protect the media encryption keys. This logical channel may be operated in any appropriately negotiated mode.
>
> The privacy (encryption) of data carried in logical channels shall be in the form specified by the OpenLogicalChannel. Transport-specific header information shall not be encrypted. The privacy of data is to be based upon end-to-end encryption.

See H.235 at 6-7.

Step (b) of claim 29 specifies: "sending a message securely from the first device to the second device."

H.323 teaches sending a message securely from the first device to the second device:

> In general, IPSEC [13/IPSEC] can be used to provide authentication and, optionally confidentiality (i.e. encryption) at the IP layer transparent to whatever (application) protocol runs above. The application protocol does not have to be updated to allow this; only security policy at each end.
>
> For example, to make maximum use of IPSEC for a simple point-to-point call, the following scenario could be followed:
>
> 1. The calling endpoint and its gatekeeper would set policy to require the use of IPSEC (authentication and, optionally, confidentiality) on the RAS protocol. Thus, before the first RAS message is sent from the endpoint to the gatekeeper, the ISAKMP/Oakley daemon on the endpoint will negotiate security services to be used on packets to and from the RAS channel's well-known port. Once negotiation is complete, the RAS channel will operate exactly as if it were not secured. Using this secure channel the gatekeeper will inform the endpoint of the address and port number of the call signaling channel in the called endpoint.
>
> 2. After obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair. Now, when the calling endpoint attempts to contact this address/port, the packets would be queued while an ISAKMP/Oakley negotiation is performed between the endpoints. Upon completion of this negotiation, an IPSEC Security Association (SA) for the address/port will exist and the Q.931 signaling can proceed.

> 3. On the Q.931 SETUP and CONNECT exchange, the endpoints can negotiate the use of IPSEC for the H.245 channel. This will allow the endpoints to again dynamically update their IPSEC policy databases to force the use of IPSEC on that connection.
>
> 4. As with the call signaling channel, a transparent ISAKMP/Oakley negotiation will take place before any H.245 packets are transmitted. The authentication performed by this ISAKMP/Oakley exchange will be the initial attempt at user-to-user authentication, and will set up a (probably) secure channel between the two users on which to negotiate the characteristics of the audio channel. If, after some person-to-person Q&A, either user is not satisfied with the authentication, different certificates can be chosen and the ISAKMP/Oakley exchange repeated.
>
> 5. After each H.245 ISAKMP/Oakley authentication, new keying material is exchanged for the RTP audio channel. This keying material is distributed by the master on the secure H.245 channel. Because the H.245 protocol is defined for the master to distribute the media keying material on the H.245 channel (to allow for multipoint communication), it is not recommended that IPSEC be used for the RTP channel.
>
> *See* H.235 at 30-31.

Security includes call establishment security, call control security, and media stream privacy, all include sending a message to the network address associated with the secure name:

> **6.3 Call establishment security**
>
> There are at least two reasons to motivate securing the call establishment channel (e.g. H.323 using Q.931). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the H-Series terminal, a secure mode of communication should be used (such as TLS/IPSEC for H.323) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.
>
> **6.4 Call control (H.245) security**
>
> The call control channel (H.245) should also be secured in some manner to provide for subsequent media privacy. The H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this, on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each endpoint. This may allow media streams to be made private for each endpoint in the conference. In order to utilize the H.245 messages in a secure manner, the entire H.245 channel (logical channel 0) should be opened in a negotiated secure manner.

The mechanism by which H.245 is made secure is dependent on the H-Series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, H.323 will utilize the H.225.0 connection signaling messages to accomplish this.

See H.235 at 6.

6.5 Media stream privacy

This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating endpoints may utilize an encrypted H.245 channel. In this manner, cryptographic algorithm selection and encryption keys as passed in the H.245 OpenLogicalChannel command are protected.

The H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy. This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity.

If it is required that the H.245 channel be operated in a non-encrypted manner, the specific media encryption keys may be encrypted separately in the manner signaled and agreed to by the participating parties. A logical channel of type h235Control may be utilized to provide the material to protect the media encryption keys. This logical channel may be operated in any appropriately negotiated mode.

The privacy (encryption) of data carried in logical channels shall be in the form specified by the OpenLogicalChannel. Transport-specific header information shall not be encrypted. The privacy of data is to be based upon end-to-end encryption.

See H.235 at 6-7.

Accordingly, H.323 anticipates claim 29 of the '181 patent under 35 U.S.C. § 102(b) above.

B. Ground No. 12: Claims 1-29 are Rendered Obvious in View of H.323, in Conjunction With H.225, H.235, and H.245, under 35 U.S.C. § 103

The Telecommunication Sector of the International Telecommunications Union (ITU-T) developed a series of recommendations that comprise the H.323 standard, which provides for secure multimedia communications in packet-based networks. The H.323 standard includes the teaching and disclosure of H.225.0, "core message definitions," H.235, "security framework," and H.245, "media channel control." As explained in **§ VIII** above, H.323 anticipates the '181 patent because the H.323 standard incorporates the teaching and disclosures of the H.225, H.235, H.245 series of recommendations. To the extent those series of recommendations are not incorporated by reference, and for the same reasons expressly described in **§ VIII (A)(1)-A(29)** with regard to anticipation, it would have been obvious to one of ordinary skill to combine the teachings of the H.323 standard with the H.225, H.235, and H.245 series of recommendations as there is an express motivation to combine those various documents because they are specifically referenced and described in the H.323 as disclosing particular features of H.323 and there are indications in H.323 that they be used together as elements of the H.323 standard.

IX. DETAILED EXPLANATION OF MANNER OF APPLYING JOHNSON TO CLAIMS 1-16 AND 18-29 AND PROPOSED REJECTIONS BASED ON GROUND NO. 13

Exhibit C6 correlates each of claims 1-16, and 18-29 of the '181 patent with the section of the present request that sets out the detailed basis for obviousness of the claim, along with an identification of the relevant portions of Johnson, in conjunction with RFC 2131, RFC 1034, and RFC 2401. Requester notes that any emphasis indicated in quotations or other citations (e.g., as shown in bold faced text) has been added and is not original to the references cited in this section, unless otherwise noted.

C. Ground No. 13: Claims 1-16 and 18-29 are Rendered Obvious in View of Johnson, in Conjunction With RFC 2131, RFC 1034, and RFC 2401, under 35 U.S.C. § 103

Johnson describes methods and systems for establishing a secure communication link between two devices across a public network such as the Internet.

1. Claim 1

Claim 1 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising":

(a) receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and

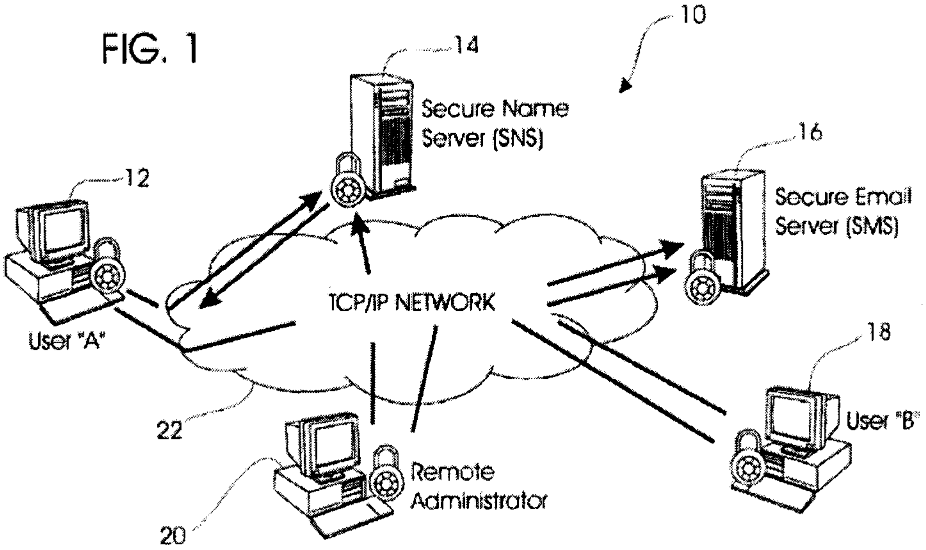
(b) sending a message over a secure communication link from the first device to the second device.

The preamble of claim 1 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name." Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. More generally, Johnson describes the disclosed invention as follows:

> The present invention is directed to an apparatus and method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:19-27.

Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "a method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like." Johnson at 1:19-27. A high-level diagram (at Figure 1) of Johnson is disclosed:

FIG. 1



Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure email server 16 registers its name with secure name server 14:

> [W]hen a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.

> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

Johnson thus teaches a secure communication network that obtains dynamic IP addresses and registers those dynamic IP addresses with a name server:

> Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22. Johnson at 6:25-35.

Johnson does not, however, specify how the dynamic address obtained by the secure electronic mail server is obtained. However, one of ordinary skill in the art understood at the time of the filing of the '181 patent how to dynamically assign IP addresses by using, for example, a Dynamic Host Configuration Protocol (DHCP) server:

> The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19]. DHCP captures the behavior of BOOTP relay agents [7, 21], and DHCP participants can interoperate with BOOTP participants [9]. RFC 2131 at 1.

DHCP, which is built on a client-server model—"where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts"—supports "three mechanisms for IP address allocation. RFC 2131 at 2-3. It would have been obvious to one of ordinary skill in the art to combine RFC 2131 with Johnson in order to implement the teachings of Johnson. RFC 2131 expressly performs the functions identified in Johnson for obtaining dynamically allocated IP addresses.

In the network described in Johnson, the secure name server 14 of Johnson—having a fixed IP address on connection network 22, *see, e.g.,* Johnson at 6:29-32—can obtain its fixed IP address automatically upon bootup through the process of "automatic allocation," in which "DHCP assigns a permanent IP address to a [DHCP] client." RFC 2131 at 3; *see also* RFC 2131 at 8. So, in RFC 2131, a DHCP client—such as secure name server 14 in Johnson—is an Internet host that uses DHCP to obtain its public IP address. RFC 2131 at 6.

The secure name server 14 of Johnson obtains its public IP address by registering its name with the DHCP server:

> DHCP defines a new 'client identifier' option that is used to pass an explicit client identifier to a DHCP server. *** The 'client identifier' is an opaque key...; for example, the 'client identifier' may contain a hardware address, identical to the contents of the 'chaddr' field, or it may contain another type of identifier, such as ***a DNS name***. The 'client identifier' chosen by a DHCP client MUST be unique to that client within the subnet to which the client is attached. If the client uses a 'client identifier' in one message, it MUST use that same identifier in all subsequent messages, to ensure that all servers correctly identify the client. RFC 2131 at 9 (emphasis added).

RFC 2131 also teaches that the DHCP client—such as secure name server 14 in Johnson—obtains from the DHCP server a "unique identifier to associate a client with its lease. The client MAY choose to explicitly provide the identifier through the 'client identifier' option. If the client supplies a 'client identifier', the client MUST use the same 'client identifier' in all subsequent messages, and the server MUST use that identifier to identify the client. *** Sites may also choose to use a DNS name as the 'client identifier', causing address leases to be associated with the DNS name rather than a specific hardware box." RFC 2131 at 26.

The client identifier for secure name server 14 is an unsecured name.

Alternatively, according to Johnson, the secure name server may be accessed or selected according to the secure name server's name. Johnson at 11:23-24 ("The process starts by selecting the target secure name server machine by its fixed address/***name*** as shown in block

150." And, Johnson further states that the invention is directed for use in communications over the Internet and interbusiness network communications:

> The invention has utility in applications such as person-to-person communication over network 25 systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:21-27.

So, in order to facilitate interbusiness or communication over the Internet using the name of the secure name server rather than the fixed IP address, it would have been obvious to have combined Johnson with RFC 1034 in order to locate the secure name server 14 by name, for example, through the public resources of the Internet. RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network over the Internet:

> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:
>
> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS ***the authoritative name server*** for the domain

RFC 1034 at 11-12 (emphasis added). Thus, the domain name in the public DNS system as necessary to the invention of Johnson also comprises an unsecured name—associated with secure name server—within the meaning of the '181 patent.

In Johnson, because the name of the secure mail server is a secure name that is registered by the secure mail server with the secure name server and has its own unique IP address, and further because the secure mail server has a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an "unsecured name," Johnson discloses "a non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name."

Step (a) of Claim 1 specifies: "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and"

The user of the invention in Johnson communicates with the secure mail server using an encrypted protocol and as such, communicates the desire to securely communicate. Johnson at 8:10-12 ("[B]ecause a communication between a user and the secure mail server 16 is protected, a second level of encryption must be broken to obtain the message.") Johnson discloses that a user (and therefore the user's device) establishes communications with another by securely communicating utilizing the invention disclosed in Johnson:

> The first user 12 now wishes to write and send an electronic mail communication to the second user 18 over the protected communication network 10. The first user 12 uses his unique logon protocol combination to access the secure name server 14 over the connecting network 22. Once again, this is a protected communication. The first user 12 then obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14. Johnson at 7:10-17.

Furthermore, Johnson explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Thus, Johnson discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Step (b) of claim 1 specifies: "sending a message over a secure communication link from the first device to the second device."

As disclosed in **steps (a)**, the user at the first device obtains a network address associated with the secure name of the second device. The user at the first device uses that network address in order to send a message to that second device utilizing the network address associated with its secure name. Johnson, at 7:20-27 (emphasis added), explains:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and **sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16**.

The message is secure because it employs encryption techniques and other protective measures in order to secure the communication:" [B]ecause the users can be using an additional protection or encryption system that is unknown to the secure networks, an additional level of protection can be used between the first user 12 and the second user 18. This additional level must also be broken to obtain the message text." Johnson at 8:9-18. Johnson further explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication

> network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Thus, Johnson discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device."

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 1 of the '181 patent under 35 U.S.C. § 103.

2. Claim 2

Independent claim 2 is directed to [a] method of using a first device to communicate with a second device having a secure name, the method comprising:

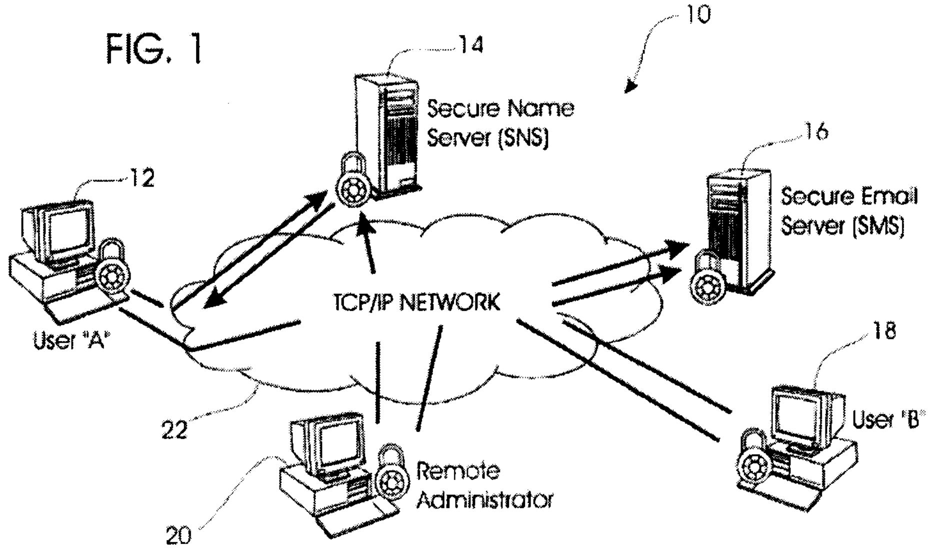
> (a) from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;
>
> (b) at the first device, receiving a message containing the network address associated with the secure name of the second device; and
>
> (c) from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

The preamble of claim 2 specifies "[a] method of using a first device to communicate with a second device having a secure name . . . ." Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. More generally, Johnson describes the disclosed invention as follows:

> The present invention is directed to an apparatus and method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:19-27.

Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "a method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like." Johnson at 1:19-27. A high-level diagram (at Figure 1) of Johnson is disclosed:

FIG. 1



Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure email server 16 registers its name with secure name server 14:

> [W]hen a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

Johnson thus teaches a secure communication network that obtains dynamic IP addresses and registers those dynamic IP addresses with a name server:

> Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22. Johnson at 6:25-35.

Johnson does not, however, specify how the dynamic address obtained by the secure electronic mail server is obtained. However, one of ordinary skill in the art understood at the time of the filing of the '181 patent how to dynamically assign IP addresses by using, for example, a Dynamic Host Configuration Protocol (DHCP) server:

> The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19]. DHCP captures the behavior of BOOTP relay agents [7, 21], and DHCP participants can interoperate with BOOTP participants [9]. RFC 2131 at 1.

DHCP, which is built on a client-server model—"where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts"—

supports "three mechanisms for IP address allocation. RFC 2131 at 2-3. It would have been obvious to one of ordinary skill in the art to combine RFC 2131 with Johnson in order to implement the teachings of Johnson. RFC 2131 expressly performs the functions identified in Johnson for obtaining dynamically allocated IP addresses.

In the network described in Johnson, the secure name server 14 of Johnson—having a fixed IP address on connection network 22, *see, e.g.,* Johnson at 6:29-32—can obtain its fixed IP address automatically upon bootup through the process of "automatic allocation," in which "DHCP assigns a permanent IP address to a [DHCP] client." RFC 2131 at 3; *see also* RFC 2131 at 8. So, in RFC 2131, a DHCP client—such as secure name server 14 in Johnson—is an Internet host that uses DHCP to obtain its public IP address. RFC 2131 at 6.

The secure name server 14 of Johnson obtains its public IP address by registering its name with the DHCP server:

> DHCP defines a new 'client identifier' option that is used to pass an explicit client identifier to a DHCP server. *** The 'client identifier' is an opaque key...; for example, the 'client identifier' may contain a hardware address, identical to the contents of the 'chaddr' field, or it may contain another type of identifier, such as ***a DNS name***. The 'client identifier' chosen by a DHCP client MUST be unique to that client within the subnet to which the client is attached. If the client uses a 'client identifier' in one message, it MUST use that same identifier in all subsequent messages, to ensure that all servers correctly identify the client. RFC 2131 at 9 (emphasis added).

RFC 2131 also teaches that the DHCP client—such as secure name server 14 in Johnson—obtains from the DHCP server a "unique identifier to associate a client with its lease. The client MAY choose to explicitly provide the identifier through the 'client identifier' option. If the client supplies a 'client identifier', the client MUST use the same 'client identifier' in all subsequent messages, and the server MUST use that identifier to identify the client. *** Sites may also choose to use a DNS name as the 'client identifier', causing address leases to be associated with the DNS name rather than a specific hardware box." RFC 2131 at 26.

The client identifier for secure name server 14 is an unsecured name.

Alternatively, according to Johnson, the secure name server may be accessed or selected according to the secure name server's name. Johnson at 11:23-24 ("The process starts by selecting the target secure name server machine by its fixed address/***name*** as shown in block 150." And, Johnson further states that the invention is directed for use in communications over the Internet and interbusiness network communications:

> The invention has utility in applications such as person-to-person communication over network 25 systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:21-27.

So, in order to facilitate interbusiness or communication over the Internet using the name of the secure name server rather than the fixed IP address, it would have been obvious to have combined Johnson with RFC 1034 in order to locate the secure name server 14 by name, for example, through the public resources of the Internet. RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network over the Internet:

> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:
>
> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS ***the authoritative name server*** for the domain

RFC 1034 at 11-12 (emphasis added). Thus, the domain name in the public DNS system as necessary to the invention of Johnson also comprises an unsecured name—associated with secure name server—within the meaning of the '181 patent.

In Johnson, because the name of the secure mail server is a secure name that is registered by the secure mail server with the secure name server and has its own unique IP address, and further that the secure name is utilized in order to securely communicate with another device, Johnson discloses "[a] method of using a first device to communicate with a second device having a secure name."

Step (a) of claim 2 further specifies: "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Johnson discloses that the a first device securely communicated with the secure name server in order to request a network address that is associated with the secure name—which is associated with the network address—of the second device, i.e., the secure mail server. At 11:21-37, Johnson explains:

> Process to Get an Address from a Secure Name Server
>
> FIG. 7 of the drawings outlines the process by which an unknown address, such as the dynamic address of a secure mail server, is obtained from a secure name server. The process starts by selecting the target secure name server machine by its fixed address/name as shown in block 150. The user then provides the secure name server with its logon protocol combination as shown at block 152. If the user logon combination is verified then a session is established with a secure name server as shown at block 154.
>
> ***

> ...if the session has been correctly established as shown at block 156, then the user will be allowed to request the address for the named machine at the client site as shown at block 158.

This process is revealed diagrammatically at Figure 7 in Johnson:

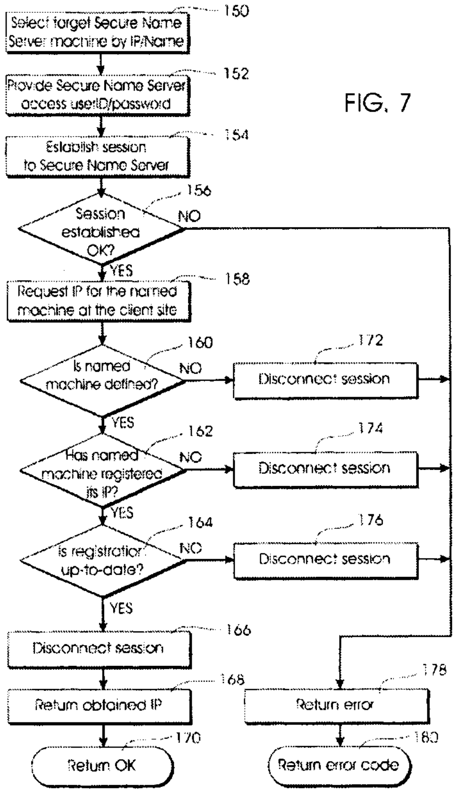

Select target Secure Name Server machine by IP/Name
150
Provide Secure Name Server access userID/password
152
Establish session to Secure Name Server
154
Session established OK?
156
NO
YES
Request IP for the named machine at the client site
158
Is named machine defined?
160
NO
Disconnect session
172
YES
Has named machine registered its IP?
162
NO
Disconnect session
174
YES
Is registration up-to-date?
164
NO
Disconnect session
176
YES
Disconnect session
166
Return obtained IP
168
Return error
178
Return OK
170
Return error code
180

FIG. 7

Thus, Johnson shows the step of "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device."

Step (b) of claim 2 further specifies: "at the first device, receiving a message containing the network address associated with the secure name of the second device; and"

As disclosed in **step (a)**, the first device requests—and subsequently receives—a network address associated with the secure name of the second device. This is further shown in Johnson by the following:

> The first user 12 now wishes to write and send an 10 electronic mail communication to the second user 18 over the protected communication network 10. The first user 12 uses his unique logon protocol combination to access the secure name server 14 over the connecting network 22. Once again, this is a protected communication. **The first user 12 then obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14.** Johnson at 7:10-17 (emphasis added).

Thus, Johnson shows the step of "at the first device, receiving a message containing the network address associated with the secure name of the second device."

Step (c) of claim 2 further specifies: "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link."

As disclosed in **steps (a)-(b)**, the user at the first device obtains a network address associated with the secure name of the second device. The user at the first device uses that network address in order to send a message to that second device utilizing the network address associated with its secure name. Johnson, at 7:20-27 (emphasis added), explains:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and **sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16.**

The message is secure because it employs encryption techniques and other protective measures in order to secure the communication:" [B]ecause the users can be using an additional protection or encryption system that is unknown to the secure networks, an additional level of protection can be used between the first user 12 and the second user 18. This additional level must also be broken to obtain the message text." Johnson at 8:9-18. Johnson further explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 2 of the '181 patent under 35 U.S.C. § 103.

3. Claim 3

Claim 3 depends from claim 2, and specifies "wherein the secure name of the second device is a secure domain name.

Johnson does not specify, for example, the names of the secure name server, the secure mail server, or the computers used by the users or the administrator registered in the secure name server, as identified above. As described in claim 1(a) above, it would have been obvious to one of ordinary skill in the art to have combined RFC 1034, titled "Doman Names – Concepts and Facilities," published by the Internet Engineering Task Force in November 1987, with Johnson in order to satisfy the stated purpose of Johnson, i.e., to facilitate communications "***over the Internet*** and ***inter-business network communications***." Johnson at 1:19-27.

RFC 1034 provides the naming conventions used to facilitate communication over the Internet and inter-business network communications, by identifying the IP addresses associated with the named computers. For example, Johnson teaches that the secure mail server registers its dynamically assigned IP address with the secure name server of protected network 10, and RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network, as it does here at 11-12:

> This RFC introduces domain style names, their use for Internet mail and host address support, and the protocols and servers used to implement domain name facilities. RFC 1034 at 1.
>
> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:
>
> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS the authoritative name server for the domain

In other words, when a user in one domain having authenticated access to the secure mail server of protected network 10 in protected network 10's domain, a DNS query can be used to obtain the IP address of the secure name server (i.e., the authoritative name server for the protected network) and, subsequently, obtain the IP address of the secure mail server for which to send the communication.

Additionally, by selecting a domain name for protected network 10 and assigning mail addresses in the format specified in RFC 1034, protected network 10, the authoritative name server residing therein, and the mailboxes corresponding to the secure mail server are easily identified:

> For mailboxes, the mapping is slightly more complex. The usual mail address <local-part>@<mail-domain> is mapped into a domain name by converting <local-part> into a single label (regardless of dots it contains), converting <mail-domain> into a domain name using the usual text format for domain names (dots denote label breaks), and concatenating the two to form a single domain name. Thus the mailbox HOSTMASTER@SRI-NIC.ARPA is represented as a domain name by HOSTMASTER.SRI-NIC.ARPA. RFC 1034 at 9.

A DNS query on the Internet for such domain name can then turn up the authoritative name server, either by specifically requesting the NS resource record or as follows:

> Using the query domain name, QTYPE, and QCLASS, the name server looks for matching RRs. In addition to relevant records, the name server may return RRs ***that point toward a name server that has the desired information***..... For example, a name server that doesn't have the requested information may know a name server that does.... RFC 1034 at 17.

Once the secure name server is identified by IP address, the remote user can query the secure name server to obtain the IP address of the secure mail server. Alternatively, a query on the mailbox name identified above, having the specified domain name, would not be found in the public DNS and the RR corresponding to the secure name server would be returned as a related RR. Together, Johnson and RFC 1034 teach, for example, that the secure name of the secure mail server can be a secure domain name.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 3 of the '181 patent under 35 U.S.C. § 103.

4. Claim 4

Claim 4 depends from claim 2, and specifies "wherein the secure name indicates security."

Johnson does not specify, for example, the names of the secure name server, the secure mail server, or the computers used by the users or the administrator registered in the secure name server, as identified above. As described in claim 1(a) above, it would have been obvious to one of ordinary skill in the art to have combined RFC 1034, titled "Doman Names – Concepts and Facilities," published by the Internet Engineering Task Force in November 1987, with Johnson in order to satisfy the stated purpose of Johnson, i.e., to facilitate communications "***over the Internet*** and ***inter-business network communications***." Johnson at 1:19-27.

RFC 1034 provides the naming conventions used to facilitate communication over the Internet and inter-business network communications, by identifying the IP addresses associated with the named computers. For example, Johnson teaches that the secure mail server registers its dynamically assigned IP address with the secure name server of protected network 10, and RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network, as it does here at 11-12:

> This RFC introduces domain style names, their use for Internet mail and host address support, and the protocols and servers used to implement domain name facilities. RFC 1034 at 1.
>
> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:

> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS the authoritative name server for the domain

In other words, when a user in one domain having authenticated access to the secure mail server of protected network 10 in protected network 10's domain, a DNS query can be used to obtain the IP address of the secure name server (i.e., the authoritative name server for the protected network) and, subsequently, obtain the IP address of the secure mail server for which to send the communication.

Additionally, by selecting a domain name for protected network 10 and assigning mail addresses in the format specified in RFC 1034, protected network 10, the authoritative name server residing therein, and the mailboxes corresponding to the secure mail server are easily identified:

> For mailboxes, the mapping is slightly more complex. The usual mail address <local-part>@<mail-domain> is mapped into a domain name by converting <local-part> into a single label (regardless of dots it contains), converting <mail-domain> into a domain name using the usual text format for domain names (dots denote label breaks), and concatenating the two to form a single domain name. Thus the mailbox HOSTMASTER@SRI-NIC.ARPA is represented as a domain name by HOSTMASTER.SRI-NIC.ARPA. RFC 1034 at 9.

A DNS query on the Internet for such domain name can then turn up the authoritative name server, either by specifically requesting the NS resource record or as follows:

> Using the query domain name, QTYPE, and QCLASS, the name server looks for matching RRs. In addition to relevant records, the name server may return RRs ***that point toward a name server that has the desired information***..... For example, a name server that doesn't have the requested information may know a name server that does.... RFC 1034 at 17.

Once the secure name server is identified by IP address, the remote user can query the secure name server to obtain the IP address of the secure mail server. Alternatively, a query on the mailbox name identified above, having the specified domain name, would not be found in the public DNS and the RR corresponding to the secure name server would be returned as a related RR. Together, Johnson and RFC 1034 teach, for example, that the secure name of the secure mail server can be a secure domain name, and because of the complexity for obtaining such a name, it indicates security.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 4 of the '181 patent under 35 U.S.C. § 103.

5. Claim 5

Claim 5 of the '181 patent depends from claim 2, and specifies "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form."

The network address of the associated with the secure name of the second device is obtained through an encrypted message. Johnson explains, at 8:4-8, for example, that "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16."

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 5 of the '181 patent under 35 U.S.C. § 103.

6. Claim 6

Claim 6 depends from claim 2, and specifies that the step of "further including decrypting the message."

As described above in Claim 5, the message containing the network address associated with the secure name of the second device in Johnson is encrypted. In order to securely communicate with the second device, the first device must decrypt the message. For example, as explained in Johnson: "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, **a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16**. Johnson at 8:4-8 (emphasis added).

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 6 of the '181 patent under 35 U.S.C. § 103.

7. Claim 7

Claim 7 of the '181 patent depends from claim 2, and specifies "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed."

Johnson discloses that the communication link between the first and second device may be a secure communication link. For example:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at [7:20-27]

Moreover, Johnson explains that it is also an embodiment of the invention to utilize unsecure communication links. Johnson at 5:45-47 ("A still further object of the present invention is to provide for a system which can communication [sic] on both secure and non-secure electronic mail servers."

Alternatively, in one embodiment—as described above in **claim 1**, for example—the secure name server resides on the same machine as the secure mail server. Johnson at 12:20-25. In such a scenario, a secure communication link would not be utilized during registration. *See* Johnson at 11:21-37; *see also* Johnson at 7:49 – 8:24(illustrating the various communications that are encrypted and, by implication, not encrypted). Thus, the second device is capable of both secure and non-secure communications.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 7 of the '181 patent under 35 U.S.C. § 103.

8. Claim 8

Claim 8 depends from claim 2 and specifies that "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure email server 16 registers its name with secure name server 14:

> [W]hen a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters

> necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

Johnson thus teaches a secure communication network that obtains dynamic IP addresses and registers those dynamic IP addresses with a name server:

> Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22. Johnson at 6:25-35.

Johnson does not, however, specify how the dynamic address obtained by the secure electronic mail server is obtained. However, one of ordinary skill in the art understood at the time of the filing of the '181 patent how to dynamically assign IP addresses by using, for example, a Dynamic Host Configuration Protocol (DHCP) server:

> The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19]. DHCP captures the behavior of BOOTP relay agents [7, 21], and DHCP participants can interoperate with BOOTP participants [9]. RFC 2131 at 1.

DHCP, which is built on a client-server model—"where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts"—supports "three mechanisms for IP address allocation. RFC 2131 at 2-3. It would have been obvious to one of ordinary skill in the art to combine RFC 2131 with Johnson in order to implement the teachings of Johnson. RFC 2131 expressly performs the functions identified in Johnson for obtaining dynamically allocated IP addresses.

As the dynamically assigned IP address is a "secure name" within the meaning of the '181 patent, Johnson thus discloses "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device."

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 8 of the '181 patent under 35 U.S.C. § 103.

9. Claim 9

Claim 9 depends from claim 2 and specifies "further including automatically initiating the secure communication link after it is enabled."

As described above, Johnson discloses the following process for securely communicating:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at [7:20-27]

While Johnson does not explicitly mention that the secure communication link is automatically initiated, it would have been inherent in such a system to automatically initiate encrypted communications, and furthermore, such automatic initiation would have been well known in the art at the time of the filing of the '181 patent.

Alternatively, Johnson is an improvement over the systems of the prior art mentioned in the background section, 1:29 – 4:67, and these systems taught automatic initiation of the secure communication links. Thus, Johnson implicitly discloses this limitation.

Alternatively, one of ordinary skill in the art would have been motivated to combine Johnson with RFC 2401, titled, "Security Architecture for the Internet Protocol," published by the Internet Engineering Task Force on November 1998, describing IPSec.

> For each of the selectors defined in Section 4.4.2, the SA entry in the SAD MUST contain the value or values which were negotiated at the time the SA was created. For the sender, these values are used to decide whether a given SA is appropriate for use with an outbound packet. RFC 2401 at 21.
>
> **4.6.2 Automated SA and Key Management**
>
> Widespread deployment and use of IPsec requires an Internet-standard, scalable, automated, SA management protocol. Such support is required to facilitate use of the anti-replay features of AH and ESP, and to accommodate on-demand creation of SAs, e.g., for user- and session-oriented keying. (Note that the notion of "rekeying" an SA actually implies creation of a new SA with a new SPI, a process that generally implies use of an automated SA/key management protocol.) RFC 2401 at 27.

One of ordinary skill in the art would have been motivated to combine the references because Johnson does not specifically identify a particular encryption protocol, and the most known or general protocol for TCP/IP communications was IPSec. Automatic initiation of SSL and/or other types of encryption techniques were also well known in the art.

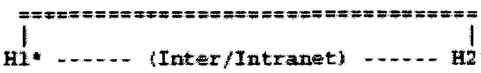
Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 9 of the '181 patent under 35 U.S.C. § 103.

10. Claim 10

Claim 10 depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link."

As described above, Johnson does not specify the type or level of obfuscation necessary in order to establish a secure communication link. However, one of ordinary skill in the art would have been motivated to combine Johnson with RFC 2401, titled, "Security Architecture for the Internet Protocol," published by the Internet Engineering Task Force on November 1998, describing IPSec, which was well known in the art to include security services that comprised, for example, a tunneling mode. RFC 2401 at 9. ("Two hosts MAY establish a tunnel mode SA between themselves."). IPSec's disclosure of a "tunneling mode" may be seen, for example, in RFC 2401 at 24-25:

> Case 1. The case of providing end-to-end security between 2 hosts across the Internet (or an Intranet).
>
> Note that either transport or tunnel mode can be selected by the hosts. So the headers in a packet between H1 and H2 could look like any of the following:



```
==================================
|                                |
H1* ------ (Inter/Intranet) ------ H2*
```

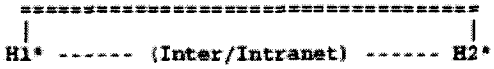
Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 10 of the '181 patent under 35 U.S.C. § 103.

11. Claim 11

Claim 11 of the '181 patent depends from claim 2, and specifies "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet."

As described above, Johnson does not specify the type or level of obfuscation necessary in order to establish a secure communication link. However, one of ordinary skill in the art would have been motivated to combine Johnson with RFC 2401, titled, "Security Architecture for the Internet Protocol," published by the Internet Engineering Task Force on November 1998, describing IPSec, which was well known in the art to include security services that comprised, for example, a tunneling mode—which would necessarily comprise receiving a message in the form of a tunneled packet. RFC 2401 at 9. ("Two hosts MAY establish a tunnel mode SA between themselves."). IPSec's disclosure of a "tunneling mode" may be seen, for example, in RFC 2401 at 24-25:

> Case 1. The case of providing end-to-end security between 2 hosts across the Internet (or an Intranet).
>
> Note that either transport or tunnel mode can be selected by the hosts. So the headers in a packet between H1 and H2 could look like any of the following:



```
==================================
|                                |
H1* ------ (Inter/Intranet) ------ H2*
```

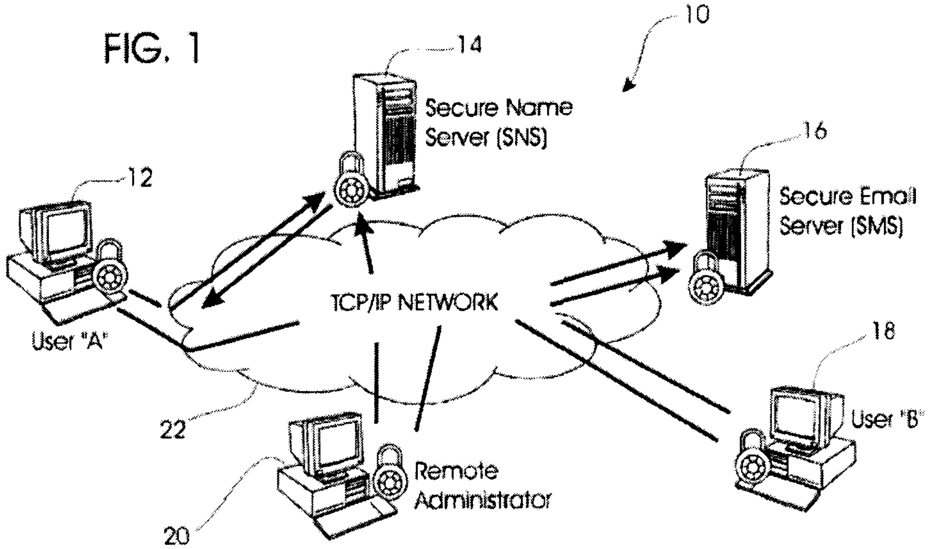
Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 11 of the '181 patent under 35 U.S.C. § 103.

12. Claim 12

Claim 12 depends from claim 2 and specifies "wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols."

The invention disclosed in Johnson would utilize a number of communications protocols, including, for example, Transmission Control Protocol and Internet Protocol—TCP/IP—in order to send and receive messages. In particular, Johnson is directed to "a method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like." Johnson at 1:19-27. A high-level diagram (at Figure 1) of Johnson is disclosed, wherein TCP/IP is disclosed:

FIG. 1



Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 12 of the '181 patent under 35 U.S.C. § 103.

13. Claim 13

Claim 13 depends from claim 2 and specifies "wherein the receiving and sending of messages through the secure communication link includes multiple sessions."

As described above, it would have been obvious to person of ordinary skill in the art to utilize the teachings of RFC 2401—and its disclosure of IPSec—in order to facilitate secure communications between devices. IPSec permits, for example, at RFC 2401 at 17, multiple sessions to traverse on a secure communication link:

> **4.4.2 Selectors**
>
> An SA (or SA bundle) may be fine-grained or coarse-grained, depending on the selectors used to define the set of traffic for the SA. For example, all traffic between two hosts may be carried via a single SA, and afforded a uniform set of security services. Alternatively, traffic between a pair of hosts might be spread over multiple SAs, depending on the applications being used (as defined by the Next Protocol and Port fields), with different security services offered by different SAs. Similarly, all traffic between a pair of security

> gateways could be carried on a single SA, or one SA could be assigned for each communicating host pair. The following selector parameters MUST be supported for SA management to facilitate control of SA granularity.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 13 of the '181 patent under 35 U.S.C. § 103.

14. Claim 14

Claim 14 depends from claim 2 and specifies "further including supporting a plurality of services over the secure communication link."

As described above, it would have been obvious to person of ordinary skill in the art to utilize the teachings of RFC 2401—and its disclosure of IPSec—in order to facilitate secure communications between devices. IPSec permits, for example, at RFC 2401 at 17, multiple sessions and, for example, different security services, to traverse on a secure communication link:

> **4.4.2 Selectors**
>
> An SA (or SA bundle) may be fine-grained or coarse-grained, depending on the selectors used to define the set of traffic for the SA. For example, all traffic between two hosts may be carried via a single SA, and afforded a uniform set of security services. Alternatively, traffic between a pair of hosts might be spread over multiple SAs, depending on the applications being used (as defined by the Next Protocol and Port fields), with different security services offered by different SAs. Similarly, all traffic between a pair of security gateways could be carried on a single SA, or one SA could be assigned for each communicating host pair. The following selector parameters MUST be supported for SA management to facilitate control of SA granularity.

Alternatively, it was known in the art that IPSec could receive and send messages that included multiple sessions through the IPSec link. RFC 2401 at 3. "This document describes the goals of such systems, their components and how they fit together with each other and into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment." The "set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols." RFC 2401 at 4.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 14 of the '181 patent under 35 U.S.C. § 103.

15. Claim 15

Claim 15 depends from claim 14 and specifies "wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof."

As described above in reference to **Claims 12-13,** Johnson supports a plurality of communication protocols and multiple sessions. Furthermore, Johnson discloses that the use of an "electronic mail program" that is used by the user in furtherance of the invention. Johnson at 10:18-21.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 14 of the '181 patent under 35 U.S.C. § 103.

16. Claim 16

Claim 16 depends from claim 15 and specifies "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof."

Johnson discloses that the use of an "electronic mail program" that is used by the user in furtherance of the invention. Johnson at 10:18-21.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 16 of the '181 patent under 35 U.S.C. § 103.

17. Claim 18

Claim 18 depends from claim 2 and specifies "wherein the secure communication link is an authenticated link."

As shown above, security is an important objective of Johnson. It would have been obvious to combine the security techniques already described in Johnson with the authentication techniques described in RFC 2401. For example:

> **2.1 Goals/Objectives/Requirements/Problem Description**
>
> IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. RFC 2401 at 4.

RFC 2401 further explains, at 10, that it "also provides authentication for selected portions of the IP header, which may be necessary in some contexts. For example, if the integrity of an IPv4 option or IPv6 extension header must be protected en route between sender and receiver, AH can provide this service (except for the non-predictable but mutable parts of the IP header)."

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, and in further view of RFC 2401, renders obvious claim 18 of the '181 patent under 35 U.S.C. § 103.

18. Claim 19

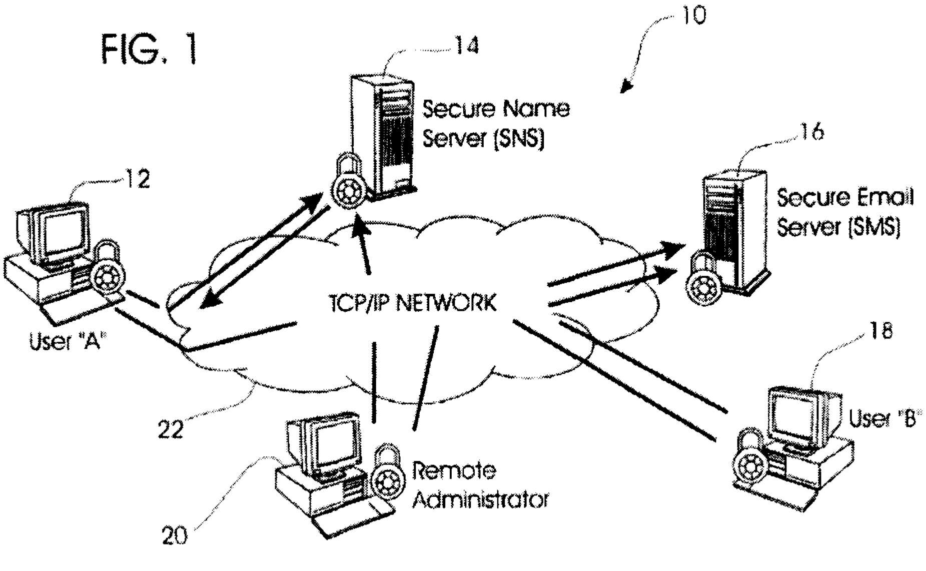
Claim 19 depends from claim 2 and specifies "wherein the first device is a computer, and the steps are performed on the computer."

Johnson discloses that the first device is a computer and that the relevant disclosed operations are performed on the first device. For example, the Abstract of Johnson describes the invention as facilitating the transfer of secure message between two devices:

> A system and method for transferring messages securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and then encrypting the message at the first device. An address for a dynamically addressed server is obtained and the first device is connected to the dynamically addressed server. The encrypted message is transmitted from the first device to the server and the message is received at the dynamically addressed server. Johnson, ABSTRACT.

The devices in Johnson are, for example, computers. Johnson at 6:17-19 ("In the preferred embodiment, the protected communication network 10 consists of ***a first central processing unit or user 12***...."). Fig. 1 also identifies item 12 as including a computer:

FIG. 1



Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 19 of the '181 patent under 35 U.S.C. § 103.

19. Claim 20

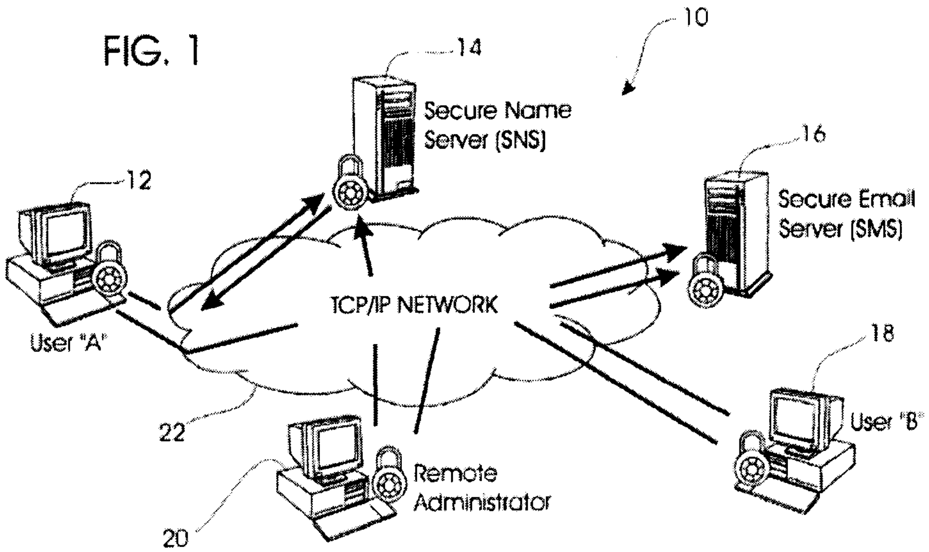
Claim 20 depends from claim 2 and specifies "wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network."

Johnson discloses that the first device is a computer and that the relevant disclosed operations are performed on the first device on the TCP/IP computer Network. For example, the Abstract of Johnson describes the invention as facilitating the transfer of secure message between two devices:

> A system and method for transferring messages securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and then encrypting the message at the first device. An address for a dynamically addressed server is obtained and the first device is connected to the dynamically addressed server. The encrypted message is transmitted from the first device to the server and the message is received at the dynamically addressed server. Johnson, ABSTRACT.

The devices in Johnson are, for example, computers. Johnson at 6:17-19 ("In the preferred embodiment, the protected communication network 10 consists of ***a first central processing unit or user 12***...."). Fig. 1 also identifies item 12 as including a computer:

FIG. 1



Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 20 of the '181 patent under 35 U.S.C. § 103.

20. Claim 21

Claim 21 depends from claim 2 and specifies "further including providing an unsecured name associated with the device."

In the network described in Johnson, the secure name server 14 of Johnson—having a fixed IP address on connection network 22, *see, e.g.,* Johnson at 6:29-32—can obtain its fixed IP address automatically upon bootup through the process of "automatic allocation," in which "DHCP assigns a permanent IP address to a [DHCP] client." RFC 2131 at 3; *see also* RFC 2131 at 8. So, in RFC 2131, a DHCP client—such as secure name server 14 in Johnson—is an Internet host that uses DHCP to obtain its public IP address. RFC 2131 at 6.

The secure name server 14 of Johnson obtains its public IP address by registering its name with the DHCP server:

> DHCP defines a new 'client identifier' option that is used to pass an explicit client identifier to a DHCP server. *** The 'client identifier' is an opaque key...; for example, the 'client identifier' may contain a hardware address, identical to the contents of the

> 'chaddr' field, or it may contain another type of identifier, such as ***a DNS name***. The 'client identifier' chosen by a DHCP client MUST be unique to that client within the subnet to which the client is attached. If the client uses a 'client identifier' in one message, it MUST use that same identifier in all subsequent messages, to ensure that all servers correctly identify the client. RFC 2131 at 9 (emphasis added).

RFC 2131 also teaches that the DHCP client—such as secure name server 14 in Johnson—obtains from the DHCP server a "unique identifier to associate a client with its lease. The client MAY choose to explicitly provide the identifier through the 'client identifier' option. If the client supplies a 'client identifier', the client MUST use the same 'client identifier' in all subsequent messages, and the server MUST use that identifier to identify the client. *** Sites may also choose to use a DNS name as the 'client identifier', causing address leases to be associated with the DNS name rather than a specific hardware box." RFC 2131 at 26.

The client identifier for secure name server 14 is an unsecured name.

Alternatively, according to Johnson, the secure name server may be accessed or selected according to the secure name server's name. Johnson at 11:23-24 ("The process starts by selecting the target secure name server machine by its fixed address/***name*** as shown in block 150." And, Johnson further states that the invention is directed for use in communications over the Internet and interbusiness network communications:

> The invention has utility in applications such as person-to-person communication over network 25 systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:21-27.

So, in order to facilitate interbusiness or communication over the Internet using the name of the secure name server rather than the fixed IP address, it would have been obvious to have combined Johnson with RFC 1034 in order to locate the secure name server 14 by name, for example, through the public resources of the Internet. RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network over the Internet:

> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:
>
> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS ***the authoritative name server*** for the domain

RFC 1034 at 11-12 (emphasis added). Thus, the domain name in the public DNS system as necessary to the invention of Johnson also comprises an unsecured name—associated with secure name server—within the meaning of the '181 patent.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 21 of the '181 patent under 35 U.S.C. § 103.

21. Claim 22

Claim 22 depends from claim 2 and specifies "wherein the secure name is registered prior to the step of sending a message to a secure name service."

Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure email server 16 registers its name with secure name server 14:

> [W]hen a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

Johnson thus teaches a secure communication network that obtains dynamic IP addresses and registers those dynamic IP addresses with a name server:

> Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22. Johnson at 6:25-35.

Johnson does not, however, specify how the dynamic address obtained by the secure electronic mail server is obtained. However, one of ordinary skill in the art understood at the time of the filing of the '181 patent how to dynamically assign IP addresses by using, for example, a Dynamic Host Configuration Protocol (DHCP) server:

> The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19]. DHCP captures the behavior of BOOTP relay agents [7, 21], and DHCP participants can interoperate with BOOTP participants [9]. RFC 2131 at 1.

DHCP, which is built on a client-server model—"where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts"—supports "three mechanisms for IP address allocation. RFC 2131 at 2-3. It would have been obvious to one of ordinary skill in the art to combine RFC 2131 with Johnson in order to implement the teachings of Johnson. RFC 2131 expressly performs the functions identified in Johnson for obtaining dynamically allocated IP addresses

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 22 of the '181 patent under 35 U.S.C. § 103.

22. Claim 23

Claim 23 depends from claim 2 and specifies "wherein the secure name of the second device is a secure, non-standard domain name."

As described above in reference to **claim 22**, for example, the secure name disclosed in Johnson is a dynamic IP address, which would not be resolvable by a Public DNS system and would therefore, be non-standard.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 22 of the '181 patent under 35 U.S.C. § 103.

23. Claim 24

Independent claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network, the method comprising:

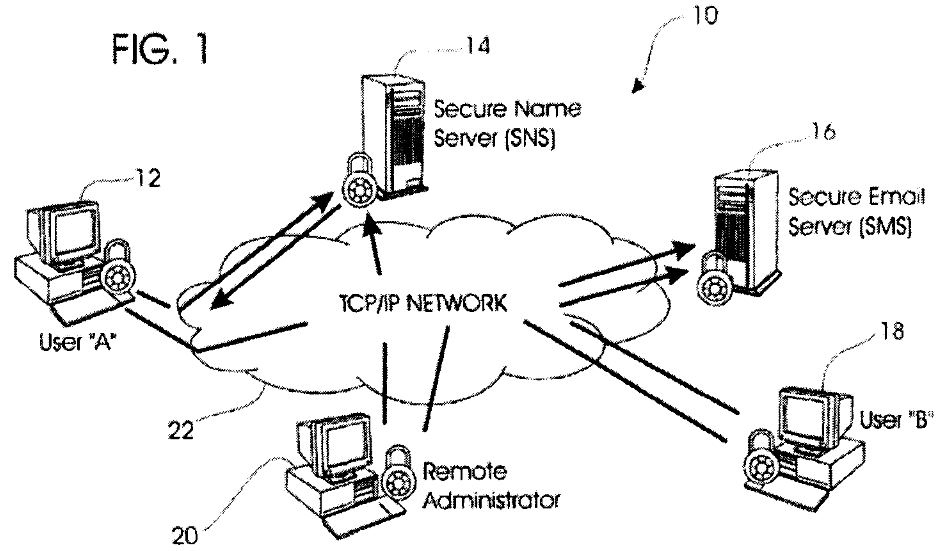
(a) at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;

(b) receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and

(c) sending a message securely from the first device to the second device."

The preamble of claim 24 is directed to "[a] method of using a first device to securely communicate with a second device over a communication network." Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. Every user, computer, administrator or server registers a secure name with a secure name server. Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "a method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like." Johnson at 1:19-27. A high-level diagram (at Figure 1) of Johnson is disclosed:

FIG. 1



Step (a) of claim 24 further specifies: "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure mail server registers its name with secure name server:

> As shown in FIG. 5, when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully

> established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

In Johnson, because the name of the secure mail server is a secure name that is registered by the secure mail server with the secure name server and has its own unique IP address, Johnson discloses "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

Step (b) of claim 24 further specifies: "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and."

A user of the invention in Johnson communicates with the secure mail server using an encrypted protocol and as such, communicates the desire to securely communicate. Johnson at 8:10-12 ("[B]ecause a communication between a user and the secure mail server 16 is protected, a second level of encryption must be broken to obtain the message.")

Step (c) of claim 24 further specifies: "sending a message securely from the first device to the second device.

Johnson explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on

> the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 24 of the '181 patent under 35 U.S.C. § 103.

24. Claim 25

Claim 25 depends from claim 24 and specifies "wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link."

Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure mail server registers its name with secure name server:

> As shown in FIG. 5, when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

In Johnson, because the name of the secure mail server is a secure name that is registered by the secure mail server with the secure name server and has its own unique IP address, Johnson discloses "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address."

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 24 of the '181 patent under 35 U.S.C. § 103.

25. Claim 26

Independent claim 26 is directed to "[a] method of using a first device to communicate with a second device over a communication network, the method comprising:

(a) from the first device requesting and obtaining registration of an unsecured name associated with the first device;

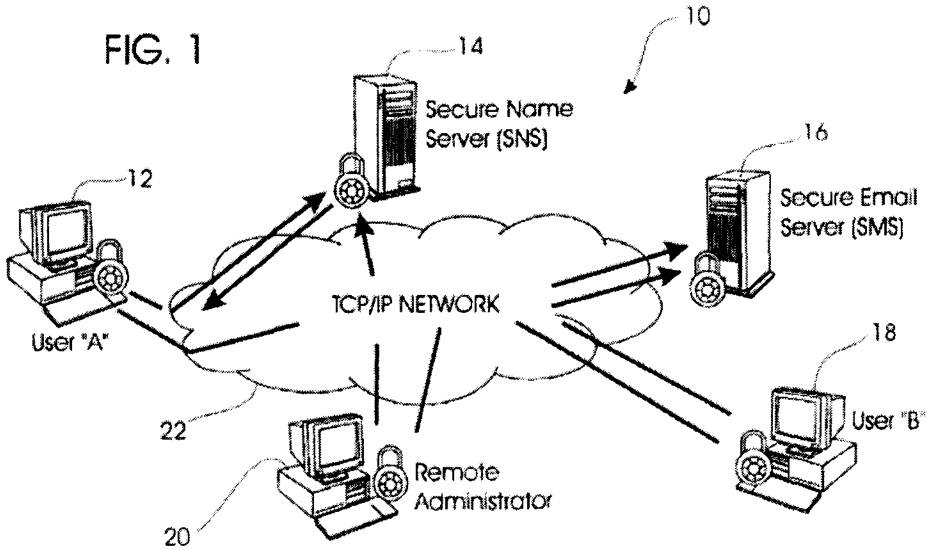
(b) from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;

(c) receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

(d) from the first device sending a message securely from the first device to the second device."

Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. Every user, computer, administrator or server registers a secure name with a secure name server. Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "a method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like." Johnson at 1:19-27. A high-level diagram (at Figure 1) of Johnson is disclosed:

FIG. 1



Step (a) of claim 26 further specifies: "from the first device requesting and obtaining registration of an unsecured name associated with the first device"

Johnson teaches, for example, at 6:25-35, a secure communication network that obtains dynamic IP addresses and registers those dynamic IP addresses with a name server:

> Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22.

Johnson does not, however, specify how the dynamic address obtained by the secure electronic mail server are obtained. One of ordinary skill in the art would have understood at the time of the filing of the '181 patent how to dynamically assign IP addresses by using, e.g., a Dynamic Host Configuration Protocol (DHCP) server, as described in RFC 2131 at 1:

> The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19]. DHCP captures the behavior of BOOTP relay agents [7, 21], and DHCP participants can interoperate with BOOTP participants [9].

DHCP is "is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. . . . and supports three mechanisms for IP address allocation." RFC 2131 at 2-3. It would have been obvious to one of ordinary skill in the art to combine RFC 2131 with Johnson in order to implement the teachings of Johnson. RFC 2131 expressly performs the functions identified in Johnson for obtaining dynamically allocated IP addresses.

In such a network, the secure name server 14 of Johnson, having a fixed IP address on connection network 22 (see, e.g., Johnson at 6:29-32), can obtain its fixed IP address automatically upon bootup. RFC 2131 at 3 (DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a [DHCP] client). RFC 2131 also explains that:

> From the client's point of view, DHCP is an extension of the BOOTP mechanism. This behavior allows existing BOOTP clients to interoperate with DHCP servers without requiring any change to the clients' initialization software. RFC 2131 at 8.

In RFC 2131, a DHCP client is an Internet host that uses DHCP to obtain its IP address. RFC 2131 at 6 ("A DHCP client is an Internet host using DHCP to obtain configuration parameters such as a network address.") The secure name server 14 of Johnson would obtain its IP address by registering its name with the DHCP server:

> DHCP defines a new 'client identifier' option that is used to pass an explicit client identifier to a DHCP server. *** The 'client identifier' is an opaque key...; for example, the 'client identifier' may contain a hardware address, identical to the contents of the 'chaddr' field, or it may contain another type of identifier, such as ***a DNS name***. The 'client identifier' chosen by a DHCP client MUST be unique to that client within the subnet to which the client is attached. If the client uses a 'client identifier' in one message, it MUST use that same identifier in all subsequent messages, to ensure that all servers correctly identify the client.

RFC 2131 at 9 (emphasis added).

> A DHCP server needs to use some unique identifier to associate a client with its lease. The client MAY choose to explicitly provide the identifier through the 'client identifier' option. If the client supplies a 'client identifier', the client MUST use the same 'client identifier' in all subsequent messages, and the server MUST use that identifier to identify the client. *** Sites may also choose to use a DNS name as the 'client identifier', causing address leases to be associated with the DNS name rather than a specific hardware box.

RFC 2131 at 26. The client identifier for secure name server 14, described above, is an unsecured name. Alternatively, according to Johnson, the secure name server may be accessed or selected according to the secure name server's name. Johnson at 11:23-25 (The process starts by selecting the target secure name server machine by its fixed address/***name*** as shown in block 150.).

In order to facilitate interbusiness or communication over the Internet using the name of the secure name server rather than the fixed IP address, it would have been obvious to have combined Johnson with RFC 1034 in order to locate the secure name server by name over, e.g., the Internet. RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network over the Internet:

> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:
>
> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS ***the authoritative name server*** for the domain

RFC 1034 at 11-12 (emphasis added). The domain name in the public DNS system comprises an unsecured name associated with the secure name server.

Thus, Johnson discloses "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Step (b) of claim 26 further specifies: "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device"

Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure mail server registers its name with secure name server:

> As shown in FIG. 5, when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for

> establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

In Johnson, because the name of the secure mail server is a secure name that is registered by the secure mail server with the secure name server and has its own unique IP address, Johnson discloses "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device."

Step (c) of claim 26 further specifies: "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and"

The user of the invention in Johnson communicates with the secure mail server using an encrypted protocol and as such, communicates the desire to securely communicate. Johnson at 8:10-12 ("[B]ecause a communication between a user and the secure mail server 16 is protected, a second level of encryption must be broken to obtain the message.")

Step (d) of claim 26 further specifies: "from the first device sending a message securely from the first device to the second device."

Johnson explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 26 of the '181 patent under 35 U.S.C. § 103.

26. Claim 27

Claim 27 depends from claim 26 and specifies:

(a) "wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

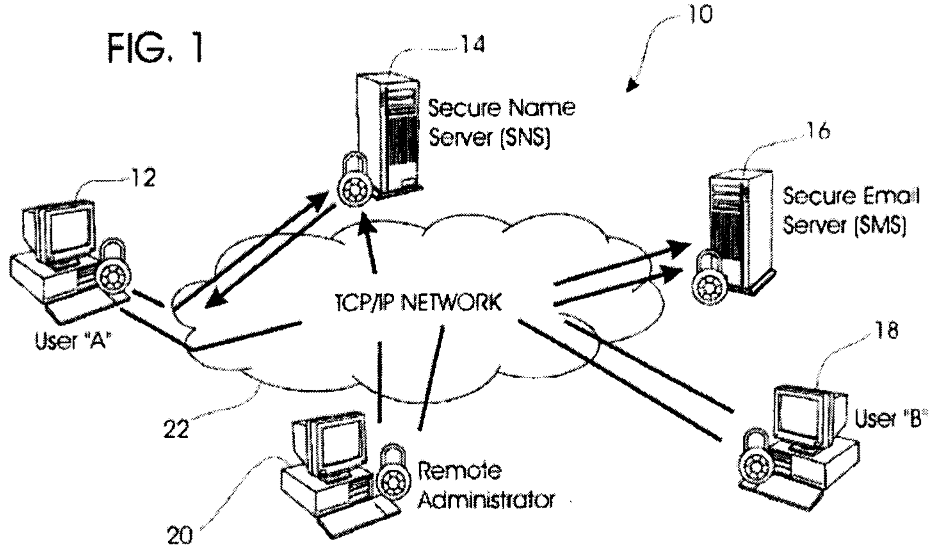
(b) wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device."

The preamble of claim 27 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name." Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. More generally, Johnson describes the disclosed invention as follows:

> The present invention is directed to an apparatus and method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:19-27.

Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "a method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like." Johnson at 1:19-27. A high-level diagram (at Figure 1) of Johnson is disclosed:

FIG. 1



Johnson teaches that secure mail server 16, seen above in Figure 1, can be on the same device as the secure name server, each being identified by separate IP addresses. Johnson at 12:20-25 (It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed [IP] address of the secure name server while providing for a dynamic [IP] address of the secure mail server.). Thus, in Johnson, the secure email server 16 registers its name with secure name server 14:

> [W]hen a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.
>
> As shown in block 120, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block 122. As shown in block 124, a session with a secure name server is then established. If the session is successfully established as shown in block 126, **then the machine will go on to register the dynamic address for the named machine 128**, disconnect the session 130, and then properly shut down this process as shown in block 134. Johnson at 10:36-52.

The name registered by the secure mail server with the secure name server is a "secure name" within the meaning of the '181 patent because it requires, for example, authorization to access and is protected through encryption, as explained by Johnson at 9:23-33:

> FIG. 3 of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start 60 by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server 62 for the dynamic address of the secure mail server. **Block 64 represents checking to see it properly obtained the dynamic address of secure mail server 20 from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server**, the user will move on connect to the mail server at block 66.

Further, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. Johnson at 8:4-9.

Johnson thus teaches a secure communication network that obtains dynamic IP addresses and registers those dynamic IP addresses with a name server:

> Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22. Johnson at 6:25-35.

Johnson does not, however, specify how the dynamic address obtained by the secure electronic mail server is obtained. However, one of ordinary skill in the art understood at the time of the filing of the '181 patent how to dynamically assign IP addresses by using, for example, a Dynamic Host Configuration Protocol (DHCP) server:

> The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the capability of automatic allocation of reusable network addresses and additional configuration options [19]. DHCP captures the behavior of BOOTP relay agents [7, 21], and DHCP participants can interoperate with BOOTP participants [9]. RFC 2131 at 1.

DHCP, which is built on a client-server model—"where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts"—supports "three mechanisms for IP address allocation. RFC 2131 at 2-3. It would have been obvious to one of ordinary skill in the art to combine RFC 2131 with Johnson in order to implement the teachings of Johnson. RFC 2131 expressly performs the functions identified in Johnson for obtaining dynamically allocated IP addresses.

In the network described in Johnson, the secure name server 14 of Johnson—having a fixed IP address on connection network 22, *see, e.g.,* Johnson at 6:29-32—can obtain its fixed IP address automatically upon bootup through the process of "automatic allocation," in which "DHCP assigns a permanent IP address to a [DHCP] client." RFC 2131 at 3; *see also* RFC 2131 at 8. So, in RFC 2131, a DHCP client—such as secure name server 14 in Johnson—is an Internet host that uses DHCP to obtain its public IP address. RFC 2131 at 6.

The secure name server 14 of Johnson obtains its public IP address by registering its name with the DHCP server:

> DHCP defines a new 'client identifier' option that is used to pass an explicit client identifier to a DHCP server. *** The 'client identifier' is an opaque key...; for example, the 'client identifier' may contain a hardware address, identical to the contents of the 'chaddr' field, or it may contain another type of identifier, such as ***a DNS name***. The 'client identifier' chosen by a DHCP client MUST be unique to that client within the subnet to which the client is attached. If the client uses a 'client identifier' in one message, it MUST use that same identifier in all subsequent messages, to ensure that all servers correctly identify the client. RFC 2131 at 9 (emphasis added).

RFC 2131 also teaches that the DHCP client—such as secure name server 14 in Johnson—obtains from the DHCP server a "unique identifier to associate a client with its lease. The client MAY choose to explicitly provide the identifier through the 'client identifier' option. If the client supplies a 'client identifier', the client MUST use the same 'client identifier' in all subsequent messages, and the server MUST use that identifier to identify the client. *** Sites may also choose to use a DNS name as the 'client identifier', causing address leases to be associated with the DNS name rather than a specific hardware box." RFC 2131 at 26.

The client identifier for secure name server 14 is an unsecured name.

Alternatively, according to Johnson, the secure name server may be accessed or selected according to the secure name server's name. Johnson at 11:23-24 ("The process starts by selecting the target secure name server machine by its fixed address/***name*** as shown in block 150." And, Johnson further states that the invention is directed for use in communications over the Internet and interbusiness network communications:

> The invention has utility in applications such as person-to-person communication over network 25 systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:21-27.

So, in order to facilitate interbusiness or communication over the Internet using the name of the secure name server rather than the fixed IP address, it would have been obvious to have combined Johnson with RFC 1034 in order to locate the secure name server 14 by name, for example, through the public resources of the Internet. RFC 1034 teaches, *inter alia*, how to identify the authoritative name server for a particular network over the Internet:

> **3.6. Resource Records**
>
> A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). ***
>
> When we talk about a specific RR, we assume it has the following:
>
> ***
>
> MX identifies a mail exchange for the domain. ***
>
> ***
>
> NS ***the authoritative name server*** for the domain

RFC 1034 at 11-12 (emphasis added). Thus, the domain name in the public DNS system as necessary to the invention of Johnson also comprises an unsecured name—associated with secure name server—within the meaning of the '181 patent.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 27 of the '181 patent under 35 U.S.C. § 103.

27. Claim 28

Independent claim 28 is directed to "[a] non-transitory machine-readable medium comprising instructions for:

(a) sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

(b) receiving a message containing the network address associated with the secure name of the device; and

(c) sending a message to the network address associated with the secure name of the device using a secure communication link.

The preamble of claim 28 specifies "[a] non-transitory machine-readable medium comprising instructions." Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. More generally, Johnson describes the disclosed invention as follows:

> The present invention is directed to an apparatus and method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over

> network systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:19-27.

Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "[a] non-transitory machine-readable medium comprising instructions."

Step (a) of claim 28 further specifies: "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;"

Johnson discloses that the a first device securely communicated with the secure name server in order to request a network address that is associated with the secure name—which is associated with the network address—of the second device, i.e., the secure mail server. At 11:21-37, Johnson explains:

> Process to Get an Address from a Secure Name Server
>
> FIG. 7 of the drawings outlines the process by which an unknown address, such as the dynamic address of a secure mail server, is obtained from a secure name server. The process starts by selecting the target secure name server machine by its fixed address/name as shown in block 150. The user then provides the secure name server with its logon protocol combination as shown at block 152. If the user logon combination is verified then a session is established with a secure name server as shown at block 154.
>
> ***
>
> ...if the session has been correctly established as shown at block 156, then the user will be allowed to request the address for the named machine at the client site as shown at block 158.

This process is revealed diagrammatically at Figure 7 in Johnson:

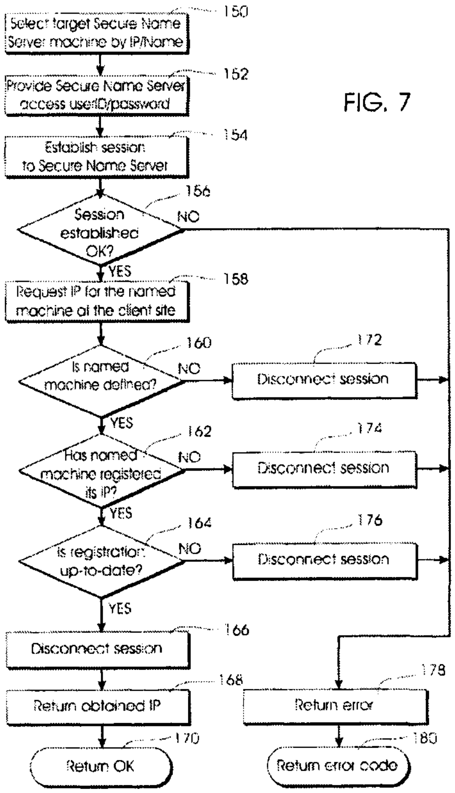

150
Select target Secure Name Server machine by IP/Name
152
Provide Secure Name Server access userID/password
154
Establish session to Secure Name Server
156
Session established OK?
NO
YES
158
Request IP for the named machine at the client site
160
Is named machine defined?
NO
172
Disconnect session
YES
162
Has named machine registered its IP?
NO
174
Disconnect session
YES
164
Is registration up-to-date?
NO
176
Disconnect session
YES
166
Disconnect session
168
Return obtained IP
170
Return OK
178
Return error
180
Return error code

FIG. 7

Step (b) of claim 28 further specifies: "receiving a message containing the network address associated with the secure name of the device; and"

As disclosed in **step (a)**, the first device requests—and subsequently receives—a network address associated with the secure name of the second device. This is further shown in Johnson by the following:

> The first user 12 now wishes to write and send an 10 electronic mail communication to the second user 18 over the protected communication network 10. The first user 12 uses his unique logon protocol combination to access the secure name server 14 over the connecting network 22. Once again, this is a protected communication. **The first user 12 then obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14.** Johnson at 7:10-17 (emphasis added).

Step (c) of claim 28 further specifies: "sending a message to the network address associated with the secure name of the device using a secure communication link."

As disclosed in **steps (a)-(b)**, the user at the first device obtains a network address associated with the secure name of the second device. The user at the first device uses that network address in order to send a message to that second device utilizing the network address associated with its secure name. Johnson, at 7:20-27 (emphasis added), explains:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the

> secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and **sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16**.

The message is secure because it employs encryption techniques and other protective measures in order to secure the communication:" [B]ecause the users can be using an additional protection or encryption system that is unknown to the secure networks, an additional level of protection can be used between the first user 12 and the second user 18. This additional level must also be broken to obtain the message text." Johnson at 8:9-18. Johnson further explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 28 of the '181 patent under 35 U.S.C. § 103.

28. Claim 29

Independent claim 29 is directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

> (a) receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and
>
> (b) sending a message securely from the first device to the second device.

The preamble of claim 29 specifies "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name." Johnson discloses systems and methods for transmitting communications "securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and the encrypting the message at the first device." Johnson, ABSTRACT. More generally, Johnson describes the disclosed invention as follows:

> The present invention is directed to an apparatus and method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like. Johnson at 1:19-27.

Johnson at 10:36-50 ("when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted" in order to "supply[] the proper dynamic address to the secure name server.") Johnson is thus directed to "[a] non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name."

Step (a) of claim 29 further specifies: "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and"

The user of the invention in Johnson communicates with the secure mail server using an encrypted protocol and as such, communicates the desire to securely communicate. Johnson at 8:10-12 ("[B]ecause a communication between a user and the secure mail server 16 is protected, a second level of encryption must be broken to obtain the message.") Johnson discloses that a user (and therefore the user's device) establishes communications with another by securely communicating utilizing the invention disclosed in Johnson:

> The first user 12 now wishes to write and send an electronic mail communication to the second user 18 over the protected communication network 10. The first user 12 uses his unique logon protocol combination to access the secure name server 14 over the connecting network 22. Once again, this is a protected communication. The first user 12 then obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14. Johnson at 7:10-17.

Step (b) of claim 29 further specifies: "sending a message securely from the first device to the second device."

Johnson explains that:

> The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. Johnson at 7:20-27.

Accordingly, Johnson, in view of RFC 2131 and RFC 1034, renders obvious claim 29 of the '181 patent under 35 U.S.C. § 103.

X. CONCLUSIONS

Based on the explanations provided herein, Requester believes that substantial new questions of patentability have been established for each of claims 1-29 of the '181 patent. Requester accordingly submits that an *inter partes* reexamination should be established, and claims 1-29 of the '181 patent should be rejected on each of the grounds specified above that establishes a substantial new question of patentability.

Requester authorizes the Director to charge any fees not already provided with this request that are determined to be required to Deposit Account No. 18-1260.

Respectfully submitted,

/ Jeffrey P. Kushan /
Jeffrey P. Kushan
Registration No. 43,401

SIDLEY AUSTIN LLP
1501 K Street, N.W
Washington, D.C. 20005

Date: March 28, 2012

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 8,051,181		)		
		)		
Filed:	February 27, 2007	)	Group Art Unit:	Central Reexamination Unit
Issued:	November 1, 2011	)		
		)	Examiner:	
Inventors:	Larson et al.	)		
		)	Confirmation No.:	
For:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)		

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

TRANSMITTAL LETTER

Transmitted herewith is a request for inter partes reexamination of United States Patent No. 8,051,181, entitled "Method for Establishing a Secure Communication Link Between Computers of Virtual Private Network," and accompanying documents listed below:

1. Request For Inter Partes Reexamination Under 35 U.S.C. § 311.
2. Form PTO/SB/42, listing each patent and printed publication relied upon to provide a substantial new question of patentability.
3. Exhibit A: copy of U.S. Patent No. 8,051,181.
4. Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311.
5. Exhibit C1: Claim Chart - Beser.
6. Exhibit C2: Claim Chart - Mattaway.
7. Exhibit C3: Claim Chart – Lendenmann.

8. Exhibit C4: Claim Chart – Provino.
9. Exhibit C5: Claim Chart – H.323.
10. Exhibit C6: Claim Chart - Johnson
11. Exhibit X1: Beser et al., U.S. Patent No. 6,496,867.
12. Exhibit X2: Mattaway et al., U.S. Patent No. 6,131,121.
13. Exhibit X3: Lendenmann, R. et al. "Understanding OSF DCE 1.1 for AIX and OS/2," IBM International Technical Support Organization (October 1995); pp.1-274.
14. Exhibit X4: Provino, J., U.S. Patent No. 6,557,037.
15. Exhibit X5: Droms, R. RFC 2131, "Dynamic Host Configuration Protocol" (November 1987); pp. 1-39.
16. Exhibit X6: Johnson, R., U.S. Patent No. 6,499,108.
17. Exhibit X7: ITU-T Recommendation H.323, "Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services. Packet-based multimedia communications systems," International Telecommunications Union (February 1998); pp.1-128.
18. Exhibit X8: ITU-T Recommendation H.225.0, "Infrastructure of audiovisual services – Transmission multiplexing and synchronization. Call signalling protocols and media stream packetization for packet-based multimedia communication systems," International Telecommunication Union (February 1998); pp. 1-155.
19. Exhibit X9: ITU-T Recommendation H.235, "Infrastructure of audiovisual services – Systems aspects. Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," International Telecommunication Union (February 1998); pp. 1-39.
20. Exhibit X10: ITU-T Recommendation H.245, "Infrastructure of audiovisual services – Communication procedures. Control protocol for multimedia communication," International Telecommunication Union (February 1998); pp. 1-280.
21. Exhibit X11: Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities" (November 1987); pp. 1-47.
22. Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58).

Please charge the amount of $8,800 in payment of the fee for the Request for Inter Partes Reexamination to Sidley Austin LLP's Deposit Account No. 18-1260. If it should be determined that additional fees are required, please charge any required fee to Sidley Austin LLP's Deposit Account No. 18-1260. Please credit any overpayment to Deposit Account No. 18-1260.

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requestor

JPK/klk
SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile
March 28, 2012

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Karen L. Knezek.
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Request for inter reexamination	1813	1	8800	8800
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**8800**

Electronic Acknowledgement Receipt

EFS ID:	12400087
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	26116
Filer:	Karen L. Knezek.
Filer Authorized By:	
Attorney Docket Number:	41484-80200
Receipt Date:	28-MAR-2012
Filing Date:	
Time Stamp:	17:07:23
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$8800
RAM confirmation Number	4283
Deposit Account	181260
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Copy of patent for which reexamination is requested	Exhibit_A_USP_8051181.pdf	5158784 12932e8e557363a6004ee23a226cb133b204e330	no	82
Warnings:					
Information:					
2	Reexam Miscellaneous Incoming Letter	Exhibit_X1_USP_6496867.pdf	2292876 a736bccba363c4c3c2004c6ee8d3d6696c120bf6	no	36
Warnings:					
Information:					
3	Reexam Miscellaneous Incoming Letter	Exhibit_X2_USP_6131121.pdf	4305835 a71b11b50815aeb7c4ef3ff69d89ec4f726c07da	no	67
Warnings:					
Information:					
4	Non Patent Literature	Exhibit_X3_Lendenmann.pdf	14245843 3627de3849fa3c9f4f2ce982063523be73cad460	no	275
Warnings:					
Information:					
5	Reexam Miscellaneous Incoming Letter	Exhibit_X4_USP_6557037.pdf	1243318 362c0d1c24dd24072fc068dbd74782b9050f0a6f	no	14
Warnings:					
Information:					
6	Non Patent Literature	Exhibit_X5_Droms_RFC_2131.pdf	2053745 2dcd9ee4a5492b737efae35acc206c15bd68dca8	no	40
Warnings:					
Information:					
7	Reexam Miscellaneous Incoming Letter	Exhibit_X6_USP_6499108.pdf	1048228 9ad14b40e643f58741ac6d51d5aeaa5816620615	no	17
Warnings:					
Information:					
8	Non Patent Literature	Exhibit_X7_ITU-T_H_323.pdf	6637823 f74c20f9a681fce43fce8f882bdf789f9ffb73cf	no	129
Warnings:					
Information:					

9	Non Patent Literature	Exhibit_X8_ITU-T_H_225_0.pdf	8760205 4180b11c0bd19a6cbfb69d31cd9d8b2969ae51de	no	156
Warnings:					
Information:					
10	Non Patent Literature	Exhibit_X9_ITU-T_H_235.pdf	2184122 f848ee92b147ef2fe3d76e1788b99afc67ccb27f	no	40
Warnings:					
Information:					
11	Non Patent Literature	Exhibit_X10_ITU-T_H_245.pdf	13296389 cef8b252dabb1419e0bdc75bb6111f70c37bfdae	no	281
Warnings:					
Information:					
12	Non Patent Literature	Exhibit_X11_Mockapetris_RFC_1034.pdf	2283871 5bed5f521e3752a5dd1161277f39a6ff8b895eab	no	48
Warnings:					
Information:					
13	Information Disclosure Statement (IDS) Form (SB08)	IDS_PTOSB42.pdf	106047 0dbad4f4edd43374b9e496f09aa21e6f957d12c3	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
14	Transmittal Letter	transmittalformsb0058.pdf	884958 cfbc1dd3ed8486d78bbceb90bd7f67a1f1d4e51c	no	2
Warnings:					
Information:					
15	Receipt of Original Inter Partes Reexam Request	Exhibit_C2_Claim_Chart_Mattaway.pdf	472841 b9a163e77e4f89ee1eaa98527c93b31ced2a50bd	no	9
Warnings:					
Information:					
16	Reexam Certificate of Service	Exhibit_B_Certificate_of_Service.pdf	60167 fae8a1418d344f8453249f564308e24e23c83d88	no	2
Warnings:					
Information:					
17	Receipt of Original Inter Partes Reexam Request	Exhibit_C6_Claim_Chart_Johnson.pdf	504139 6d24fb0d8d52a6e42977228d8a851b9430663d9d	no	10

Warnings:					
Information:					
18	Receipt of Original Inter Partes Reexam Request	Exhibit_C1_Claim_Chart_Beser.pdf	474205 040444c90b618b02b60e493f119653cbbb85c6f1	no	9
Warnings:					
Information:					
19	Receipt of Original Inter Partes Reexam Request	Exhibit_C3_Claim_Chart_Lendenmann.pdf	477369 52c71d63ea148a62d45547fdd52721b3fbc59d04	no	9
Warnings:					
Information:					
20	Receipt of Original Inter Partes Reexam Request	Exhibit_C4_Claim_Chart_Provino.pdf	474239 7601d3ff35548de3a4595308681d90731ed82ab7	no	9
Warnings:					
Information:					
21	Receipt of Original Inter Partes Reexam Request	Exhibit_C5_Claim_Chart_H_323.pdf	465625 0aa49668897ada11b7f4a1a6a8358876aecbda64	no	9
Warnings:					
Information:					
22	Receipt of Original Inter Partes Reexam Request	Request_for_Inter_Partes_Reexamination.pdf	18693279 2412d963d1e780d73cc447e495c865ee93712346	no	319
Warnings:					
Information:					
23	Transmittal Letter	Transmittal_Letter.pdf	70888 344808d20f4527ee17ae6951edd02115d12a9069	no	3
Warnings:					
Information:					
24	Fee Worksheet (SB06)	fee-info.pdf	29935 9b9b54334472205af9ea4a899e467f2061f8461d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	86224731		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

EXHIBIT A

U.S. PATENT 8,051,181

US008051181B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,051,181 B2**
(45) **Date of Patent: *Nov. 1, 2011**

(54) **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx, Inc.**, Scotts Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 183 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/679,416**

(22) Filed: **Feb. 27, 2007**

(65) **Prior Publication Data**

US 2008/0005792 A1 Jan. 3, 2008

Related U.S. Application Data

(60) Division of application No. 09/558,209, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/227**; 709/228

(58) **Field of Classification Search** 709/225–229, 709/245
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Garland Roper Charles et al.
4,920,484	A	4/1990	Ranade
4,933,846	A	6/1990	Humphrey et al.
4,988,990	A	1/1991	Warrior
5,164,988	A	11/1992	Matyas
5,276,735	A	1/1994	Boebert et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	199 24 575	12/1999

(Continued)

OTHER PUBLICATIONS

Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.

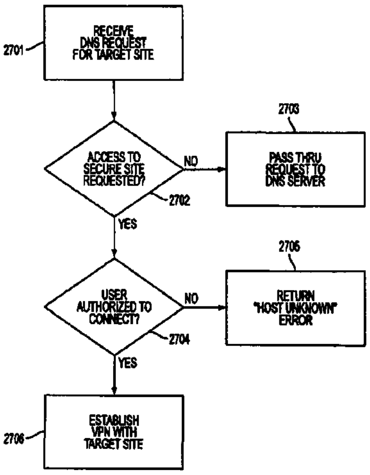
(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

29 Claims, 40 Drawing Sheets


RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
2702
NO
PASS THRU REQUEST TO DNS SERVER
2703
YES
USER AUTHORIZED TO CONNECT?
2704
NO
RETURN "HOST UNKNOWN" ERROR
2705
YES
ESTABLISH VPN WITH TARGET SITE
2706

U.S. PATENT DOCUMENTS

5,303,302	A	4/1994	Burrows
5,311,593	A	5/1994	Carmi
5,329,521	A	7/1994	Walsh et al.
5,341,426	A	8/1994	Barney et al.
5,367,643	A	11/1994	Chang et al.
5,384,848	A	1/1995	Kikuchi
5,511,122	A	4/1996	Atkinson
5,559,883	A	9/1996	Williams
5,561,669	A	10/1996	Lenney et al.
5,588,060	A	12/1996	Aziz
5,590,285	A	12/1996	Krause et al.
5,625,626	A	4/1997	Umekita
5,629,984	A	5/1997	McManis
5,654,695	A	8/1997	Olnowich et al.
5,682,480	A	10/1997	Nakagawa
5,689,566	A	11/1997	Nguyen
5,740,375	A	4/1998	Dunne et al.
5,764,906	A	6/1998	Edelstein et al.
5,771,239	A	6/1998	Moroney et al.
5,774,660	A	6/1998	Brendel et al.
5,787,172	A	7/1998	Arnold
5,790,548	A	8/1998	Sistanizadeh et al.
5,796,942	A	8/1998	Esbensen
5,805,801	A	9/1998	Holloway et al.
5,805,803	A	9/1998	Birrell et al.
5,822,434	A	10/1998	Caronni et al.
5,842,040	A	11/1998	Hughes et al.
5,845,091	A	12/1998	Dunne et al.
5,864,666	A	1/1999	Shrader
5,867,650	A	2/1999	Osterman
5,870,610	A	2/1999	Beyda et al.
5,878,231	A	3/1999	Baehr et al.
5,892,903	A	4/1999	Klaus
5,898,830	A	4/1999	Wesinger et al.
5,905,859	A	5/1999	Holloway et al.
5,918,018	A	6/1999	Gooderum et al.
5,918,019	A	6/1999	Valencia
5,950,195	A	9/1999	Stockwell et al.
5,996,016	A	11/1999	Thalheimer et al.
6,006,259	A	12/1999	Adelman et al.
6,006,272	A	12/1999	Aravamudan et al.
6,016,318	A	1/2000	Tomoike
6,016,512	A	1/2000	Huitema
6,041,342	A	3/2000	Yamaguchi
6,052,788	A	4/2000	Wesinger et al.
6,055,574	A	4/2000	Smorodinsky et al.
6,061,346	A	5/2000	Nordman
6,061,736	A	5/2000	Rochberger et al.
6,079,020	A	6/2000	Liu
6,081,900	A	6/2000	Subramaniam et al.
6,092,200	A	7/2000	Muniyappa et al.
6,101,182	A	8/2000	Sistanizadeh et al.
6,119,171	A	9/2000	Alkhatib
6,119,234	A	9/2000	Aziz et al.
6,147,976	A	11/2000	Shand et al.
6,157,957	A	12/2000	Berthaud
6,158,011	A	12/2000	Chen et al.
6,168,409	B1	1/2001	Fare
6,173,399	B1	1/2001	Gilbrech
6,175,867	B1	1/2001	Taghadoss
6,178,409	B1	1/2001	Weber et al.
6,178,505	B1	1/2001	Schneider et al.
6,179,102	B1	1/2001	Weber et al.
6,199,112	B1	3/2001	Wilson
6,202,081	B1	3/2001	Naudus
6,222,842	B1	4/2001	Sasyan et al.
6,223,287	B1	4/2001	Douglas et al.
6,226,748	B1	5/2001	Bots et al.
6,226,751	B1	5/2001	Arrow et al.
6,233,618	B1	5/2001	Shannon
6,243,360	B1	6/2001	Basilico
6,243,749	B1	6/2001	Sitaraman et al.
6,243,754	B1	6/2001	Guerin et al.
6,246,670	B1	6/2001	Karlsson et al.
6,256,671	B1	7/2001	Strentzsch et al.
6,262,987	B1	7/2001	Mogul
6,263,445	B1	7/2001	Blumenau
6,286,047	B1	9/2001	Ramanathan et al.
6,298,341	B1	10/2001	Mann et al.
6,301,223	B1	10/2001	Hrastar et al.
6,308,213	B1	10/2001	Valencia
6,308,274	B1	10/2001	Swift
6,311,207	B1	10/2001	Mighdoll et al.
6,314,463	B1	11/2001	Abbott et al.
6,324,161	B1	11/2001	Kirch
6,330,562	B1	12/2001	Boden et al.
6,332,158	B1	12/2001	Risley et al.
6,333,272	B1	12/2001	McMillin et al.
6,338,082	B1	1/2002	Schneider
6,353,614	B1	3/2002	Borella et al.
6,425,003	B1	7/2002	Herzog et al.
6,430,155	B1	8/2002	Davie et al.
6,430,610	B1	8/2002	Carter
6,487,598	B1	11/2002	Valencia
6,502,135	B1	12/2002	Munger et al.
6,505,232	B1	1/2003	Mighdoll et al.
6,510,154	B1	1/2003	Mayes et al.
6,549,516	B1	4/2003	Albert et al.
6,557,037	B1	4/2003	Provino
6,571,296	B1	5/2003	Dillon
6,571,338	B1	5/2003	Shaio et al.
6,581,166	B1	6/2003	Hirst et al.
6,606,708	B1	8/2003	Devine et al.
6,618,761	B2	9/2003	Munger et al.
6,671,702	B2	12/2003	Kruglikov et al.
6,687,551	B2	2/2004	Steindl
6,687,746	B1	2/2004	Shuster et al.
6,701,437	B1	3/2004	Hoke et al.
6,714,970	B1	3/2004	Fiveash et al.
6,717,949	B1	4/2004	Boden et al.
6,751,738	B2	6/2004	Wesinger, Jr. et al.
6,752,166	B2	6/2004	Lull et al.
6,757,740	B1	6/2004	Parekh et al.
6,760,766	B1	7/2004	Sahlqvist
6,826,616	B2	11/2004	Larson et al.
6,839,759	B2	1/2005	Larson et al.
6,937,597	B1	8/2005	Rosenberg et al.
7,010,604	B1	3/2006	Munger et al.
7,039,713	B1	5/2006	Van Gunter et al.
7,072,964	B1	7/2006	Whittle et al.
7,133,930	B2	11/2006	Munger et al.
7,167,904	B1	1/2007	Devarajan et al.
7,188,175	B1	3/2007	McKeeth
7,188,180	B2	3/2007	Larson et al.
7,197,563	B2	3/2007	Sheymov et al.
7,353,841	B2	4/2008	Kono et al.
7,461,334	B1	12/2008	Lu et al.
7,490,151	B2	2/2009	Munger et al.
7,493,403	B2	2/2009	Shull et al.
2001/0049741	A1	12/2001	Skene et al.
2002/0004898	A1	1/2002	Droge
2003/0196122	A1	10/2003	Wesinger, Jr. et al.
2004/0199493	A1	10/2004	Ruiz et al.
2004/0199520	A1	10/2004	Ruiz et al.
2004/0199608	A1	10/2004	Rechterman et al.
2004/0199620	A1	10/2004	Ruiz et al.
2005/0055306	A1	3/2005	Miller et al.
2006/0059337	A1	3/2006	Poyhonen et al.
2007/0208869	A1	9/2007	Adelman et al.
2007/0214284	A1	9/2007	King et al.
2007/0266141	A1	11/2007	Norton
2008/0235507	A1	9/2008	Ishikawa et al.

FOREIGN PATENT DOCUMENTS

EP	0838930		4/1988
EP	0 814 589		12/1997
EP	0814589		12/1997
EP	0 838 930		4/1998
EP	836306		4/1998
EP	836306	A1	4/1998
EP	0 858 189		8/1998
GB	2 317 792		4/1998
GB	2317792		4/1998
GB	2 334 181	A	8/1999
GB	2334181		8/1999
GB	2340702		2/2000
JP	62-214744		9/1987

JP	04-363941	12/1992
JP	09-018492	1/1997
JP	10-070531	3/1998
WO	WO 98/27783	6/1998
WO	WO98/27783	6/1998
WO	WO 9827783 A	6/1998
WO	WO9843396	10/1998
WO	WO 98 55930	12/1998
WO	WO 98 59470	12/1998
WO	WO99/11019	3/1999
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/17775	3/2000
WO	WO 01/17775	3/2000
WO	WO 00/70458	11/2000
WO	WO 01/16766	3/2001
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Microsoft Corporation's Fifth Amended Invalidity Contentions dated Sep. 18, 2009, *VirnetX Inc. and Science Applications International Corp.* v. *Microsoft Corporation* and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759.

The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (Nov. 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.

Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (Nov. 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (Jul. 1996) ("Galvin").

WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000).

WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999).

WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000).

WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (Feb. 2000).

WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14, 2000) (resubmitted).

WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes* (Jul. 21, 2000).

DNS-related correspondence dated Sep. 7, 1993 to Sep. 20, 1993. (Pre KX, KX Records).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 2, 1996). (RFC 2543 Internet Draft 1).

Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail).

Aventail Corp., "Socks Version 5," Aventail Whitepaper, available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Mar. 27, 1997). (RFC 2543 Internet Draft 2).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 31, 1997). (RFC 2543 Internet Draft 3).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 11, 1997). (RFC 2543 Internet Draft 4).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (May 14, 1998). (RFC 2543 Internet Draft 5).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jun. 17, 1998). (RFC 2543 Internet Draft 6).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 16, 1998). (RFC 2543 Internet Draft 7).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Aug. 7, 1998). (RFC 2543 Internet Draft 8).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Sep. 18, 1998). (RFC 2543 Internet Draft 9).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 12, 1998). (RFC 2543 Internet Draft 10).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 15, 1998). (RFC 2543 Internet Draft 11).

Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail).

Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail).

Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail).

Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jan. 15, 1999). (RFC 2543 Internet Draft 12).

Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW).

Assured Digital Products. (Assured Digital).

F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3).

F-Secure, *F-Secure Evaluation Kit* (Sep. 1998) (FSECURE 00000009) (Evaluation Kit 9).

IRE, Inc., *SafeNet/Soft-PK Version 4* (Mar. 28, 2000) (Soft-PK Version 4).

IRE/SafeNet Inc., *VPN Technologies Overview* (Mar. 28, 2000) (Safenet VPN Overview).

IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager).

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000).

David Kosiur, "Building and Managing Virtual Private Networks" (1998).

P. Mockapetris, "Domain Names—Implementation and Specification," Network Working Group, RFC 1035 (Nov. 1987).

Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.

Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.

Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998).

D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, Dec. 5, 1958, First Edition, first copy, p. 102-108.

Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998).

Chapman et al., "Domain Name System (DNS)," 278-296 (1995).

Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), vol. 1729; 85-102 (1999).

De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999).

Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998).

Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pp. 122-131 (1999).

Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000).

Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pp. 399-440 (1999).

Takata, "U.S. Vendors Take Serious Action to Act Against Crackers—A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87 (1997).

Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998).

PCT International Search Report for related PCT Application No. PCT/US01/13261, 8 pages.

PCT International Search Report for related PCT Application No. PCT/US99/25323, 3 pages.

PCT International Search Report for related PCT Application No. PCT/US99/25325, 3 pages.

Non-Final Office Action dated Jun. 16, 2003 from corresponding U.S. Appl. No. 09/429,643.

Final Office Action dated Feb. 11, 2004 from corresponding U.S. Appl. No. 09/429,643.

Notice of Allowance dated May 27, 2009 from corresponding U.S. Appl. No. 11/839,969.

Non-Final Office Action dated Mar. 1, 2004 from corresponding U.S. Appl. No. 10/401,888.

Non-Final Office Action dated May 4, 2004 from corresponding U.S. Appl. No. 09/429,643.

Non-Final Office Action dated Jun. 24, 2004 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Jul. 21, 2004 from corresponding U.S. Appl. No. 10/401,888.

Notice of Allowance dated Aug. 16, 2004 from corresponding U.S. Appl. No. 10/702,580.

Notice of Allowance dated Aug. 17, 2004 from corresponding U.S. Appl. No. 10/702,522.

Non-Final Office Action dated Oct. 21, 2004 from corresponding U.S. Appl. No. 10/401,551.

Final Office Action dated Apr. 11, 2005 from corresponding U.S. Appl. No. 09/429,643.

Non-Final Office Action dated Jun. 3, 2005 from corresponding U.S. Appl. No. 10/401,551.

Notice of Allowance dated Aug. 10, 2005 from corresponding U.S. Appl. No. 09/429,643.

Non-Final Office Action dated Oct. 18, 2005 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Dec. 5, 2005 from corresponding U.S. Appl. No. 09/429,643.

Final Office Action dated Dec. 7, 2005 from corresponding U.S. Appl. No. 10/401,551.

Notice of Allowance dated Feb. 16, 2006 from corresponding U.S. Appl. No. 10/401,551.

Notice of Allowance dated Mar. 17, 2006 from corresponding U.S. Appl. No. 10/401,551.

Non-Final Office Action dated Mar. 28, 2006 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Apr. 5, 2006 from corresponding U.S. Appl. No. 10/401,551.

Notice of Allowance dated Apr. 18, 2006 from corresponding U.S. Appl. No. 10/401,551.

Notice of Allowance dated May 9, 2006 from corresponding U.S. Appl. No. 10/401,551.

Non-Final Office Action dated May 19, 2006 from corresponding U.S. Appl. No. 10/702,486.

Non-Final Office Action dated Oct. 30, 2006 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Nov. 21, 2006 from corresponding U.S. Appl. No. 10/702,486.

Non-Final Office Action dated Mar. 21, 2007 from corresponding U.S. Appl. No. 10/714,849.

Non-Final Office Action dated Jun. 15, 2007 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Oct. 29, 2007 from corresponding U.S. Appl. No. 10/714,849.

Notice of Allowance dated Jan. 11, 2008 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Apr. 10, 2008 from corresponding U.S. Appl. No. 10/714,849.

Notice of Allowance dated Jul. 1, 2008 from corresponding U.S. Appl. No. 10/259,494.

Non-Final Office Action dated Sep. 17, 2008 from corresponding U.S. Appl. No. 11/839,969.

Deposition Transcript for Gary Tomlinson dated Feb. 27, 2009.

Non-Final Office Action dated Mar. 5, 2009 from corresponding U.S. Appl. No. 11/301,022.

Notice of Allowance dated Apr. 3, 2009 from corresponding U.S. Appl. No. 11/839,969.

Non-Final Office Action dated Jun. 9, 2009 from corresponding U.S. Appl. No. 11/839,987.

Non-Final Office Action dated Sep. 2, 2009 from corresponding U.S. Appl. No. 11/924,460.

Notice of Allowance dated Sep. 16, 2009 from corresponding U.S. Appl. No. 11/839,969.

Notice of Allowance dated Nov. 19, 2009 from corresponding U.S. Appl. No. 11/839,969.

Final Office Action dated Jan. 6, 2010 from corresponding U.S. Appl. No. 11/839,987.

Notice of Allowance dated Jan. 13, 2010 from corresponding U.S. Appl. No. 11/839,969.

Notice of Allowance dated Jan. 28, 2010 from corresponding U.S. Appl. No. 11/840,508.

Final Office Action dated Feb. 9, 2010 from corresponding U.S. Appl. No. 11/301,022.

Notice of Allowance dated Feb. 24, 2010 from corresponding U.S. Appl. No. 11/839,987.

Non-Final Office Action dated Mar. 19, 2010 from corresponding U.S. Appl. No. 11/840,560.

Non-Final Office Action dated Jun. 7, 2010 from corresponding U.S. Appl. No. 11/924,460.

Non-Final Office Action dated Jun. 9, 2010 from corresponding U.S. Appl. No. 11/924,460.

Non-Final Office Action dated Jul. 1, 2010 from corresponding U.S. Appl. No. 11/839,969.

Non-Final Office Action dated Jul. 8, 2010 from corresponding U.S. Appl. No. 11/839,987.

Non-Final Office Action dated Jul. 14, 2010 from corresponding U.S. Appl. No. 11/840,508.

Final Office Action dated Oct. 21, 2010 from corresponding U.S. Appl. No. 11/840,560.

Non-Final Office Action dated Dec. 14, 2010 from corresponding U.S. Appl. No. 11/839,937.

Notice of Allowance dated Jan. 4, 2011 from corresponding U.S. Appl. No. 11/301,022.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 10, 2010, 9:00 AM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 10, 2010, 1:00 PM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 11, 2010, 9:00 AM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 11, 2010, 1:30 PM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 12, 2010, 9:00 AM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 12, 2010, 1:15 PM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 15, 2010, 9:00 AM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 15, 2010, 12:35 PM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 8, 2010, 8:45 AM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 8, 2010, 1:30 PM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 9, 2010, 9:00 AM.

Trial Transcript, *VirnetX* vs. *Microsoft Corporation* dated Mar. 9, 2010, 1:30 PM.

European Search Report dated Jan. 24, 2011 from corresponding European Application No. 10011949.4.

European Search Report dated Mar. 17, 2011 from corresponding European Application No. 10184502.2.

Hollenbeck et al., Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999).

Notice of Allowance dated Mar. 14, 2011 from corresponding U.S. Appl. No. 11/840,508.

Tannenbaum, “Computer Networks,” pp. 202-219 (1996).

Defendants' Preliminary Joint Invalidity Contentions dated Jul. 1, 2011.

Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated Jul. 1, 2011.

Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated Jul. 1, 2011.

Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the '211 Patent[2].

Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the '504 Patent[2].

Exhibit 3, RFC 2543[1] vs. Claims of the '135 Patent[2].

Exhibit 4, RFC 2543[1] vs. Claims of the '211 Patent[2].

Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent[2].

Exhibit 6, SIP Draft v.2[1] vs. Claims of the '135 Patent[2].

Exhibit 7, SIP Draft v.2[1] vs. Claims of the '211 Patent[2].

Exhibit 8, SIP Draft v.2[1] vs. Claims of the '504 Patent[2].

Exhibit 9, H.323[1] vs. Claims of the '135 Patent[2].

Exhibit 10, H.323[1] vs. Claims of the '211 Patent[2].

Exhibit 11, H.323[1] vs. Claims of the '504 Patent[2].

Exhibit 12, SSL 3.0[1] vs. Claims of the '135 Patent[2].

Exhibit 13, SSL 3.0[1] vs. Claims of the '211 Patent[2].

Exhibit 14, SSL 3.0[1] vs. Claims of the '504 Patent[2].

Exhibit 15, RFC 2487[1] vs. Claims of the '135 Patent[2].

Exhibit 16, RFC 2487[1] vs. Claims of the '211 Patent[2].

Exhibit 17, RFC 2487[1] vs. Claims of the '504 Patent[2].

Exhibit 18, RFC 2595[1] vs. Claims of the '135 Patent[2].

Exhibit 19, RFC 2595[1] vs. Claims of the '211 Patent[2].

Exhibit 20, RFC 2595[1] vs. Claims of the '504 Patent[2].

Exhibit 21, iPass[1] vs. Claims of the '135 Patent[2].

Exhibit 22, iPASS[1] vs. Claims of the '211 Patent[2].

Exhibit 23, iPASS[1] vs. Claims of the '504 Patent[2].

Exhibit 24, “US '034”[1] vs. Claims of the '135 Patent[2].

Exhibit 25, US Patent No. 6,453,034 (“US '034”)[1] vs. Claims of the '211 Patent[2].

Exhibit 26, US Patent No. 6,453,034 (“US '034”)[1] vs. Claims of the '504 Patent[2].

Exhibit 27, US '287[1] vs. Claims of the '135 Patent[2].

Exhibit 28, US '287[1] vs. Claims of the '211 Patent[2].

Exhibit 29, US '287[1] vs. Claims of the '504 Patent[2].

Exhibit 30, Overview of Access VPNs[1] vs. Claims of the '135 Patent[2].

Exhibit 31, Overview of Access VPNs[1] vs. Claims of the '211 Patent[2].

Exhibit 32, Overview of Access VPNs[1] vs. Claims of the '504 Patent[2].

Exhibit 34, RFC 1928[1] vs. Claims of the '135 Patent[2].

Exhibit 35, RFC 1928[1] vs. Claims of the '211 Patent[2].

Exhibit 36, RFC 1928[1] vs. Claims of the '504 Patent[2].

Exhibit 37, RFC 2661[1] vs. Claims of the '135 Patent[2].

Exhibit 38, RFC 2661[1] vs. Claims of the '211 Patent[2].

Exhibit 39, RFC 2661[1] vs. Claims of the '504 Patent[2].

Exhibit 40, SecureConnect[1] vs. Claims of the '135 Patent[2].

Exhibit 41, SecureConnect[1] vs. Claims of the '211 Patent[2].

Exhibit 42,SecureConnect[1] vs. Claims of the '504 Patent[2].

Exhibit 43, SFS-HTTP[1] vs. Claims of the '135 Patent[2].

Exhibit 44, SFS-HTTP[1] vs. Claims of the '211 Patent[2].

Exhibit 45, SFS-HTTP[1] vs. Claims of the '504 Patent[2].

Exhibit 46, US '883[1] vs. Claims of the '135 Patent[2].

Exhibit 47, US '883[1] vs. Claims of the '211 Patent[2].

Exhibit 48, US '883[1] vs. Claims of the '504 Patent[2].

Exhibit 49, US '132[1] vs. Claims of the '135 Patent[2].

Exhibit 50, US '132[1] vs. Claims of the '211 Patent[2].

Exhibit 51, US '132[1] vs. Claims of the '504 Patent[2].

Exhibit 52, US '213[1] vs. Claims of the '135 Patent[2].

Exhibit 53, US '213[1] vs. Claims of the '211 Patent[2].

Exhibit 54, US '213[1] vs. Claims of the '504 Patent[2].

Exhibit 55, B&M VPNs[1] vs. Claims of the '135 Patent[2].

Exhibit 56, B&M VPNs[1] vs. Claims of the '211 Patent[2].

Exhibit 57, B&M VPNs[1] vs. Claims of the '504 Patent[2].

Exhibit 58, BorderManager[1] vs. Claims of the '135 Patent[2].

Exhibit 59, BorderManager[1] vs. Claims of the '211 Patent[2].

Exhibit 60, BorderManager[1] vs. Claims of the '504 Patent[2].

Exhibit 61, Prestige 128 Plus[1] vs. Claims of the '135 Patent[2].

Exhibit 62, Prestige 128 Plus[1] vs. Claims of the '211 Patent[2].

Exhibit 63, Prestige 128 Plus[1] vs. Claims of the '504 Patent[2].

Exhibit 64, RFC 2401[1] vs. Claims of the '135 Patent[2].

Exhibit 65, RFC 2401[1] vs. Claims of the '211 Patent[2].

Exhibit 66, RFC 2401[1] vs. Claims of the '504 Patent[2].

Exhibit 67, RFC 2486[1] vs. Claims of the '135 Patent[2].

Exhibit 68, RFC 2486[1] vs. Claims of the '211 Patent[2].

Exhibit 69, RFC 2486[1] vs. Claims of the '504 Patent[2].

Exhibit 70, Understanding IPSec[1] vs. Claims of the '135 Patent[2].

Exhibit 71, Understanding IPSec[1] vs. Claims of the '211 Patent[2].

Exhibit 72, Understanding IPSec[1] vs. Claims of the '504 Patent[2].

Exhibit 73, US '820[1] vs. Claims of the '135 Patent[2].

Exhibit 74, US '820[1] vs. Claims of the '211 Patent[2].

Exhibit 75, US '820[1] vs. Claims of the '504 Patent[2].

Exhibit 76, US '019[1] vs. Claims of the '211 Patent[2].

Exhibit 77, US '019[1] vs. Claims of the '504 Patent[2].

Exhibit 78, US '049[1] vs. Claims of the '135 Patent[2].

Exhibit 79, US '049[1] vs. Claims of the '211 Patent[2].

Exhibit 80, US '049[1] vs. Claims of the '504 Patent[2].

Exhibit 81, US '748[1] vs. Claims of the '135 Patent[2].

Exhibit 82, US '261[1] vs. Claims of the '135 Patent[2].

Exhibit 83, US '261[1] vs. Claims of the '211 Patent[2].

Exhibit 84, US '261[1] vs. Claims of the '504 Patent[2].

Exhibit 85, US '900[1] vs. Claims of the '135 Patent[2].

Exhibit 86, US '900[1] vs. Claims of the '211 Patent[2].

Exhibit 87, US '900[1] vs. Claims of the '504 Patent[2].

Exhibit 88, US '671[1] vs, Claims of the '135 Patent[2].

Exhibit 89, US '671[1] vs. Claims of the '211 Patent[2].

Exhibit 90, US '671[1] vs. Claims of the '504 Patent[2].

Exhibit 91, JP '704[1] vs. Claims of the '135 Patent[2].

Exhibit 92, JP '704[1] vs. Claims of the '211 Patent[2].

Exhibit 93, JP '704[1] vs. Claims of the '504 Patent[2].

Exhibit 94, GB '841[1] vs. Claims of the '135 Patent[2].

Exhibit 95, GB '841[1] vs. Claims of the '211 Patent[2].

Exhibit 96, GB '841[1] vs. Claims of the '504 Patent[2].

Exhibit 97, US '318[1] vs. Claims of the '135 Patent[2].

Exhibit 98, US '318[1] vs. Claims of the '211 Patent[2].

Exhibit 99, US '318[1] vs. Claims of the '504 Patent[2].

Exhibit 100, VPN/VLAN[1] vs. Claims of the '135 Patent[2].

Exhibit 101, Nikkei[1] vs. Claims of the '135 Patent[2].

Exhibit 102, Nikkei[1] vs. Claims of the '211 Patent[2].

Exhibit 103, Nikkei[1] vs. Claims of the '504 Patent[2].

Exhibit 104, Special Anthology[1] vs. Claims of the '135 Patent[2].

Exhibit 105, Omron[1] vs. Claims of the '135 Patent[2].

Exhibit 106, Gauntlet System[1] vs. Claims of the '135 Patent[2].

Exhibit 107, Gauntlet System[1] vs. Claims of the '151 Patent[2].

Exhibit 108, Gauntlet System[1] vs. Claims of the '180 Patent[2].

Exhibit 109, Gauntlet System[1] vs. Claims of the '211 Patent[2].

Exhibit 110, Gauntlet System[1] vs. Claims of the '504 Patent[2].

Exhibit 111, Gauntlet System[1] vs. Claims of the '759 Patent[2].

Exhibit 112, IntraPort System[1] vs. Claims of the '135 Patent[2].

Exhibit 113, IntraPort System[1] vs. Claims of the '151 Patent[2].

Exhibit 114, IntraPort System[1] vs. Claims of the '180 Patent[2].

Exhibit 115, IntraPort System[1] vs. Claims of the '211 Patent[2].

Exhibit 116, IntraPort System[1] vs. Claims of the '504 Patent[2].

Exhibit 117, IntraPort System[1] vs. Claims of the '759 Patent[2].

Exhibit 118, Altiga VPN System[1] vs. Claims of the '135 Patent[2].

Exhibit 119, Altiga VPN System[1] vs. Claims of the '151 Patent[2].

Exhibit 120, Altiga VPN System[1] vs. Claims of the '180 Patent[2].

Exhibit 121, Altiga VPN System[1] vs. Claims of the '211 Patent[2].

Exhibit 122, Altiga VPN System[1] vs. Claims of the '504 Patent[2].

Exhibit 123, Altiga VPN System[1] vs. Claims of the '759 Patent[2].

Exhibit 124, Kiuchi[1] vs. Claims of the '135 Patent[2].

Exhibit 125, Kiuchi[1] vs. Claims of the '151 Patent[2].

Exhibit 126, Kiuchi[1] vs. Claims of the '180 Patent[2].

Exhibit 127, Kiuchi[1] vs. Claims of the '211 Patent[2].

Exhibit 128, Kiuchi[1] vs. Claims of the '504 Patent[2].

Exhibit 129, Kiuchi[1] vs. Claims of the '759 Patent[2].

Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '135 Patent[2].

Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '151 Patent[2].

Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '180 Patent[2].

Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '211 Patent[2].

Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '504 Patent[2].

Exhibit 135, Overview[1] vs. Claims of the '759 Patent[2].

Exhibit 136, RFC 2401[1] vs. Claims of the '759 Patent[2].

Exhibit 137, Schulzrinne[1] vs. Claims of the '135 Patent[2].

Exhibit 138, Schulzrinne[1] vs. Claims of the '151 Patent[2].

Exhibit 139, Schulzrinne[1] vs. Claims of the '180 Patent[2].

Exhibit 140, Schulzrinne[1] vs. Claims of the '211 Patent[2].

Exhibit 141, Schulzrinne[1] vs. Claims of the '504 Patent[2].

Exhibit 142, Schulzrinne[1] vs. Claims of the '759 Patent[2].

Exhibit 143, Solana[1] vs. Claims of the '135 Patent[2].

Exhibit 144, Solana[1] vs. Claims of the '151 Patent[2].

Exhibit 145, Solana[1] vs. Claims of the '180 Patent[2].

Exhibit 146, Solana[1] vs. Claims of the '211 Patent[2].

Exhibit 147, Solana[1] vs. Claims of the '504 Patent[2].

Exhibit 148, Solana[1] vs. Claims of the '759 Patent[2].

Exhibit 149, Atkinson[1] vs. Claims of the '135 Patent[2].

Exhibit 150, Atkinson[1] vs. Claims of the '151 Patent[2].

Exhibit 151, Atkinson[1] vs. Claims of the '180 Patent[2].

Exhibit 152, Atkinson[1] vs. Claims of the '211 Patent[2].

Exhibit 153, Atkinson[1] vs. Claims of the '504 Patent[2].

Exhibit 154, Atkinson[1] vs. Claims of the '759 Patent[2].

Exhibit 155, Marino[1] vs. Claims of the '135 Patent[2].

Exhibit 156, Marino[1] vs. Claims of the '151 Patent[2].

Exhibit 157, Marino[1] vs. Claims of the '180 Patent[2].

Exhibit 158, Marino[1] vs. Claims of the '211 Patent[2].

Exhibit 159, Marino[1] vs. Claims of the '504 Patent[2].

Exhibit 160, Marino[1] vs. Claims of the '759 Patent[2].

Exhibit 161, Aziz ('646)[1] vs. Claims of the '759 Patent[2].

Exhibit 162, VVesinger[1] vs. Claims of the '135 Patent[2].

Exhibit 163, Wesinger[1] vs. Claims of the '151 Patent[2].

Exhibit 164, Wesinger[1] vs. Claims of the '180 Patent[2].

Exhibit 165, Wesinger[1] vs. Claims of the '211 Patent[2].

Exhibit 166, Wesinger[1] vs. Claims of the '504 Patent[2].

Exhibit 167, Wesinger[1] vs. Claims of the '759 Patent[2].

Exhibit 168, Aziz ('234)[1] vs. Claims of the '135 Patent[2].

Exhibit 169, Aziz ('234)[1] vs. Claims of the '151 Patent[2].

Exhibit 170, Aziz ('234)[1] vs. Claims of the '180 Patent[2].

Exhibit 171, Aziz ('234)[1] vs. Claims of the '211 Patent[2].

Exhibit 172, Aziz ('234)[1] vs. Claims of the '504 Patent[2].

Exhibit 173, Aziz ('234)[1] vs. Claims of the '759 Patent[2].

Exhibit 174, Schneider[1] vs. Claims of the '759 Patent[2].

Exhibit 175, Valencia[1] vs. Claims of the '135 Patent[2].

Exhibit 176, Valencia[1] vs. Claims of the '151 Patent[2].

Exhibit 177, Valencia[1] vs. Claims of the '180 Patent[2].

Exhibit 178, Valencia[1] vs. Claims of the '211 Patent[2].

Exhibit 179, Valencia[1] vs. Claims of the '504 Patent[2].

Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867[1] vs. Claims of the '180 Patent [2].

Exhibit 181, Davison[1] vs. Claims of the '135 Patent[2].

Exhibit 182, Davison[1] vs. Claims of the '151 Patent[2].

Exhibit 183, Davison[1] vs. Claims of the '180 Patent[2].

Exhibit 184, Davison[1] vs. Claims of the '211 Patent[2].

Exhibit 185, Davison[1] vs. Claims of the '504 Patent[2].

Exhibit 186, Davison[1] vs. Claims of the '759 Patent[2].

Exhibit 187, AutoSOCKS v2.1[1] vs. Claims of the '135 Patent[2].

Exhibit 188, AutoSOCKS v2.1[1] vs. Claims of the '151 Patent[2].

Exhibit 189, AutoSOCKS v2.1 Administrator's Guide[1] vs. Claims of the '180 Patent[2].

Exhibit 190, AutoSOCKS[1] vs. Claims of the '759 Patent[2].

Exhibit 191, Aventail Connect 3.01/2.51[1] vs. Claims of the '135 Patent[2].

Exhibit 192, Aventail Connect v3.01/2.51[1] vs. Claims of the '151 Patent[2].

Exhibit 193, Aventail Connect 3.01/2.51[1] vs. Claims of the '180 Patent[2].

Exhibit 194, Aventail Connect 3.01/2.51[1] vs. Claims of the '759 Patent[2].

Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the '135 Patent[2].

Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the '151 Patent[2].

Exhibit 197, Aventail Connect 3.1/2.6[1] vs. Claims of the '180 Patent[2].

Exhibit 198, Aventail Connect 3.1/2.6[1] vs. Claims of the '759 Patent[2].

Exhibit 199, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the '151 Patent[2].

Exhibit 200, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the '135 Patent[2].

Exhibit 201, BinGO! vs. Claims of the '180 Patent[2].

Exhibit 202, BinGO! vs. Claims of the '759 Patent[2].

Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0)[1] vs. Claims of the '135 Patent[2].

Exhibit 204, Domain Name System (DNS) Security[1] vs. Claims of the '211 Patent[2].

Exhibit 205, Domain Name System (DNS) Security[1] vs. Claims of the '504 Patent[2].

Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '211 Patent[2].

Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '504 Patent[2].

Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2].

Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2].

Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the '504 Patent[2].

Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the '211 Patent[2].

Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '135 Patent[2].

Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '135 Patent[2].

Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '151 Patent[2].

Exhibit 215, U.S. Patent No. 6,643,701[1] vs. Claims of the '135 Patent[2].

Exhibit 216, U.S. Patent No. 6,643,701[1] vs. Claims of the '151 Patent[2].

Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401[1] vs. Claims of the '151 Patent[2].

Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401[1] vs. Claims of the '135 Patent[2].

Exhibit 219, U.S. Patent No. 6,496,867[1] vs. Claims of the '211 Patent[2].

Exhibit 220, U.S. Patent No. 6,496,867[1] vs. Claims of the '504 Patent[2].

Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '151 Patent[2].

Exhibit 222, U.S. Patent No. 6,557,037[1] vs. Claims of the '211 Patent[2].

Exhibit 223, U.S. Patent No. 6,557,037[1] vs. Claims of the '504 Patent[2].

Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '135 Patent[2].

Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '151 Patent[2].

Exhibit Cisco-1, Cisco's Prior Art Systems[1] vs. Claims of the '135 Patent.

Exhibit Cisco-2, Cisco's Prior Art Systems[1] vs. Claims of the '151 Patent.

Exhibit Cisco-3, Cisco's Prior Art Systems[1] vs. Claims of the '180 Patent.

Exhibit Cisco-4, Cisco's Prior Art Systems[1] vs. Claims of the '211 Patent.

Exhibit Cisco-5, Cisco's Prior Art Systems[1] vs. Claims of the '504 Patent.

Exhibit Cisco-6, Cisco's Prior Art Systems[1] vs. Claims of the '759 Patent.

Exhibit Cisco-7, Cisco's Prior Art PIX System[1] vs. Claims of the '759 Patent.

Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.

August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.

D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.

D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.

Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Workshop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-66695-B, retrieved from the Internet: URL: http://www. springerlink. com/content/4uac0tb0hecoma89/fulltext.pdf> (Abstract).

Dolev, Shlomi and Ostrovsky, Rafil, Efficient Anonymous Multicast and Reception (Extended Abstract), 16 pages.

Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", Internet Draft, Apr. 1998, pp. 1-51.

F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.

Glossary for the Linux FreeS/WAN project, printed from http:// liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary. html on Feb. 21, 2002, 25 pages.

J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1. 3/doc/rationale.html on Feb. 21, 2002, 4 pages.

James E. Bellaire, "New Statement of Rules—Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.

Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.

Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.

Linux FreeS/WAN Index File, printed from http://liberty.freewan. org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.

P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.

Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.

RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP).

RFC 2543-SIP (dated Mar. 1999): Session Initiation Protocol (SIP or SIPS).

Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.

Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.

Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.

Search Report, IPER (dataed Nov. 13, 2002), International Applicatoin No. PCT/US01/04340.

Search Report, IPER (dated Feb. 6, 2002), International Application No. PCT/US01/13261.

Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.

Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NY 1986.

Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.

W. Stallings, "Cryptography and Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.

U.S. Appl. No. 60/134,547, filed May 17, 1999, Victor Sheymov.

U.S. Appl. No. 60/151,563, filed Aug. 31, 1999, Bryan Whittles.

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, *VirnetX Inc. and Science Applications International Corp.* v. *Microsoft Corporation.*

Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.

Concordance Table for the References Cited in Tables on pp. 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.

1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (Apr. 1989) (RFC1101, DNS SRV).

DNS-related correspondence dated Sep. 7, 1993 to Sep. 20, 1993. (Pre KX, KX Records).

R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (Aug. 5, 1993). (Atkinson NRL, KX Records).

Henning Schulzrinne, *Personal Mobility for Multimedia Services in the Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96).

Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology).

"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (Mar. 1996). (Safe Surfing, Website Art).

Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing).

"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (Jun. 1996). (IPSec Minutes, FreeS/WAN).

J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, Jul. 1996. (Galvin, DNSSEC).

J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (Aug. 1996). (Gilmore DNS, FreeS/WAN).

H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (Aug. 1996-Sep. 1996). (Orman DNS, FreeS/WAN).

Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (Oct. 1996). (RFC 2052, DNS SRV).

Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (Nov. 18, 1996). (SSL, Underlying Security Technology).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 2, 1996). (RFC 2543 Internet Draft 1).

M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing).

Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista.

Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX).

Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX).

Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail).

Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail).

Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail).

Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail).

Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* htto://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail).

Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail).

Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing).

Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology).

Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology).

Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology).

Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology).

Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology).

J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista).

Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (Mar. 12, 1997). (Doraswamy).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Mar. 27, 1997). (RFC 2543 Internet Draft 2).

Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication for Internet and Intranet Communication," Press Release, Apr. 3, 1997. (Secure Authentication, Aventail).

D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (Apr. 15, 1997). (Analysis, Underlying Security Technologies).

Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX).

Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX).

Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," Jun. 2, 1997. (First VPN, Aventail).

Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (Jun. 2, 1997). (Syverson, Onion Routing).

Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (Jun. 16, 1997). (AIAG Requirements, ANX).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 31, 1997). (RFC 2543 Internet Draft 3).

R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (Nov. 1997). (RFC 2230, KX Records).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 11, 1997). (RFC 2543 Internet Draft 4).

1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology).

Microsoft Corp., *Virtual Private Networking an Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology).

Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology).

"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV).

Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, Jan. 19, 1998. (VPN V2.6, Aventail).

R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, Feb. 6, 1998. (Moskowitz).

H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, vol. 2 (Mar. 29-Apr. 2, 1998). (Gateway, Schulzrinne).

C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP).

DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (May 14, 1998). (RFC 2543 Internet Draft 5).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jun. 17, 1998). (RFC 2543 Internet Draft 6).

D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (Jul. 1998). (RFC 2367).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 16, 1998). (RFC 2543 Internet Draft 7).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Aug. 7, 1998). (RFC 2543 Internet Draft 8).

Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (Aug. 18, 1998). (Focus, Microsoft Prior Art VPN Technology).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Sep. 18, 1998). (RFC 2543 Internet Draft 9).

Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (Nov. 1998). (RFC 2401, Underlying Security Technologies).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 12, 1998). (RFC 2543 Internet Draft 10) 9.

Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (Dec. 1998). (DNSSEC-7).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 15, 1998). (RFC 2543 Internet Draft 11).

Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail).

Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail).

Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail).

Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN References).

Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, Underlying Security Technologies).

Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW).

Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services* (*DNS SRV*), <draft-ieft-dnsind-frc2052bis-02.txt> (Jan. 1999). (Gulbrandsen 99, DNS SRV).

C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jan. 15, 1999). (RFC 2543 Internet Draft 12).

Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (Jan. 28, 1999). (Goldschlag III, Onion Routing).

H. Schulzrinne, "Internet Telephony: architecture and protocols—an IETF perspective," Computer Networks, vol. 31, No. 3 (Feb. 1999). (Telephony, Schulzrinne).

M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (Dec. 1996-Mar. 1999). (Handley, RFC 2543).

FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (Mar. 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN).

Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX).

Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (Jun. 21, 1999). (Hornstein, DNS SRV).

Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (Oct. 1999). (Bhattcharya LDAP VPN).

B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (Oct. 15, 1999). (Patel).

Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW).

"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan. 2000). (FirstVPN Microsoft).

Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services* (*DNS SRV*), IETF RFC 2782 (Feb. 2000). (RFC 2782, DNS SRV).

MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (Feb. 2000). (MITRE, SIPRNET).

H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, vol. 4, No. 3. pp. 47-57 (Jul. 2000). (Application, SIP).

Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (Jun. 2001). (DARPA, VPN Systems).

ANX 101: Basic ANX Service Outline. (Outline, ANX).

ANX 201: Advanced ANX Service. (Advanced, ANX).

Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX).

Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail).

Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET).

Data Fellows F-Secure VPN+ (F-Secure VPN+).

Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET).

Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing).

Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET).

SPARTA "Dynamic Virtual Private Network." (Sparta, VPN Systems).

Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET).

Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN).

Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec).

Network Associates *Gauntlet Firewall for Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide—Unix, Firewall Products).

Network Associates *Gauntlet Firewall for Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide—NT, Firewall Products).

Network Associates *Gauntlet Firewall for Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products).

Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (Mar. 19, 1999) (Gauntlet Unix Release Notes, Firewall Products).

Network Associates *Gauntlet Firewall for Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products).

Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products).

Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN).

Network Associates *Gauntlet Firewall for UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN).

Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN).

Darrell Kindred *Dynamic Virtual Private Networks* (*DVPN*) (Dec. 21, 1999) (Kindred DVPN, DVPN).

Dan Sterne et.al. *TIS Dynamic Security Perimeter Research Project Demonstration* (Mar. 9, 1998) (Dynamic Security Perimeter, DVPN).

Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (Jan. 5, 2000) (Kindred DVPN Capability, DVPN) 11.

Oct. 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN).

James Just & Dan Sterne *Security Quickstart Task Update* (Feb. 5, 1997) (Security Quickstart, DVPN).

Virtual Private Network Demonstration dated Mar. 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN).

GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration* (*IFD*) *1.1 Plan* (Mar. 10, 1998) (IFD 1.1, DVPN).

Microsoft Corp. Windows NT Server Product Documentation: Administration Guide—Connection Point Services, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.ms px (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)

Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide—Connection Manager, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

Microsoft Corp. Autodial Heuristics, available at http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft

Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) available at http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I).

Marc Levy, COM Internet Services (Apr. 23, 1999), available at http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy).

Markus Horstmann and Mary Kirtland, DCOM Architecture (Jul. 23, 1997), available at http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann).

Microsoft Corp., DCOM: A Business Overview (Apr. 1997), available at http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I).

Microsoft Corp., DCOM Technical Overview (Nov. 1996), available at http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I).

Microsoft Corp., DCOM Architecture White Paper (1998) available in PDC DVD-ROM (DCOM Architecture).

Microsoft Corp, DCOM—The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) available in PDC DVD-ROM (DCOM Business Overview II).

Microsoft Corp., DCOM—Cariplo Home Banking Over the Internet White Paper (Microsoft 1996) available in PDC DVD-ROM (Cariplo II).

Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) available in PDC DVD-ROM (DCOM Solutions in Action).

Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) available 12 in PDC DVD-ROM (DCOM Technical Overview II).

125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) available at http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy).

126. Aaron Skonnard, *Essential Winlnet* 313-423 (Addison Wesley Longman 1998) (Essential Winlnet).

Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) available at http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP).

Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.ms px (Internet Connection Services I).

Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, available athttp://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II).

Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide—Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development).

Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., Jan. 15, 1999)(Mastering Windows NT Server).

Hands on, Self-Paced Training for Supporting Version 4.0 371-473 (Microsoft Press 1998) (Hands on).

Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx. (MS PPTP).

Kenneth Gregg, et al., *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg).

Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access).

Microsoft Corp., Understanding PPTP (Windows NT 4.0), available at http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).

Microsoft Corp., Windows NT 4.0: Virtual Private Networking, available at http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing).

Microsoft Corp., Chapter 1—Introduction to Windows NT Routing with Routing and Remote Access Service, Available at http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13.

Microsoft Corp., Windows NT Server Product Documentation: Chapter 5—Planning for Large-Scale Configurations, available at http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3).

F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3).

F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3).

F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3).

F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3).

F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3).

F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6).

F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6).

F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6).

F-Secure, *F-Secure Evaluation Kit* (Sep. 1998) (FSECURE 00000009) (Evaluation Kit 9).

F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sep. 1998) (from FSECURE 00000009) (SSH Guide 9).

F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sep. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9).

F-Secure, *F-Secure VPN+* (Sep. 1998) (from FSECURE 00000009) (VPN+ Guide 9).

F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools).

F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide).

SafeNet, Inc., *VPN Policy Manager* (Jan. 2000) (VPN Policy Manager).

F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+).

IRE, Inc., *SafeNet/Soft-PK Version 4* (Mar. 28, 2000) (Soft-PK Version 4).

IRE/SafeNet Inc., *VPN Technologies Overview* (Mar. 28, 2000) (Safenet VPN Overview).

IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (Jun. 22, 1999) (Safenet Addendum).

IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (Mar. 30, 2000) (VPN Policy Manager System Description).

IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager).

IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager).

Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (Jul. 22, 1996) (Gauntlet Functional Summary).

Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall).

Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79.

Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers).

Bernard Aboba et al., *Securing L2TP using IPSEC* (Feb. 2, 1999).

156. *Finding Your Way Through the VPN Maze* (1999) ("PGP").

Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview).

TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep").

WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14, 2000).

WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (Jul. 21, 2000).

Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106* (*Contract No. F30602-98-C-0012*) (Jan. 29, 1998).

GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (Sep. 21, 1998).

BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (Mar. 16-Apr. 30, 1998).

DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint.*

GTE Internetworking, *Contractor's Program Progress Report* (Mar. 16-Apr. 30, 1998).

Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (Jan. 30, 2001).

Virtual Private Networking Countermeasure Characterization (Mar. 30, 2000).

Virtual Private Network Demonstration (Mar. 21, 1998).

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000).

Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000).

NAI Labs, *IFE 3.1 Integration Demo* (2000).

Information Assurance, *Science Fair Agenda* (2000).

Darrell Kindred et al., *Proposed Threads for IFE 3.1* (Jan. 13, 2000).

IFE 3.1 Technology Dependencies (2000).

IFE 3.1 Topology (Feb. 9, 2000).

Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (Jan. 10-11, 2000).

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000).

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000).

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000).

T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (Aug. 1, 1999) (VPNA).

Network Associates Products—*PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999).

Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology).

David Johnson et. al., *A Guide to Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology).

Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology).

Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology).

Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology).

M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology).

David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology).

John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology).

Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN).

Network Associates *Gauntlet Firewall for UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN).

File History for U.S. Appl. No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date Aug. 31, 2000.

AutoSOCKS v2.1, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html.

Ran Atkinson, *Use of DNS to Distribute Keys*, Sep. 7, 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html.

FirstVPN Enterprise Networks, Overview.

Chapter 1: Introduction to Firewall Technology, Administration Guide; Dec. 19, 2007, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062.

The TLS Protocol Version 1.0; Jan. 1999; p. 65 of 71.

Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.

Virtual Private Networks—Assured Digital Incorporated—ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm.

Accessware—The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html.

Extended System Press Release, Sep. 2, 1997; *Extended VPN Uses the Internet to Create Virtual Private Networks*, www.extendedsystems.com.

Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html.

Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sep. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com.

Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing.

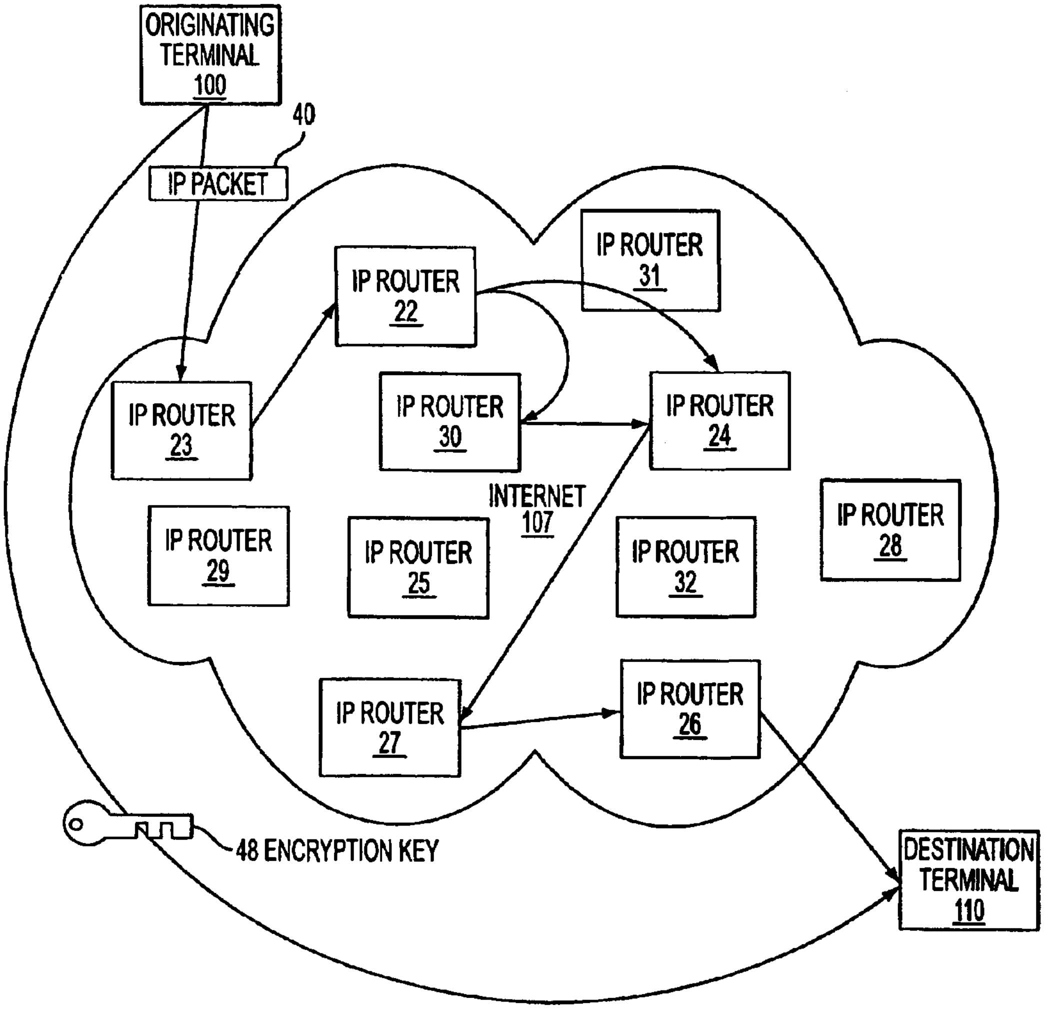

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1

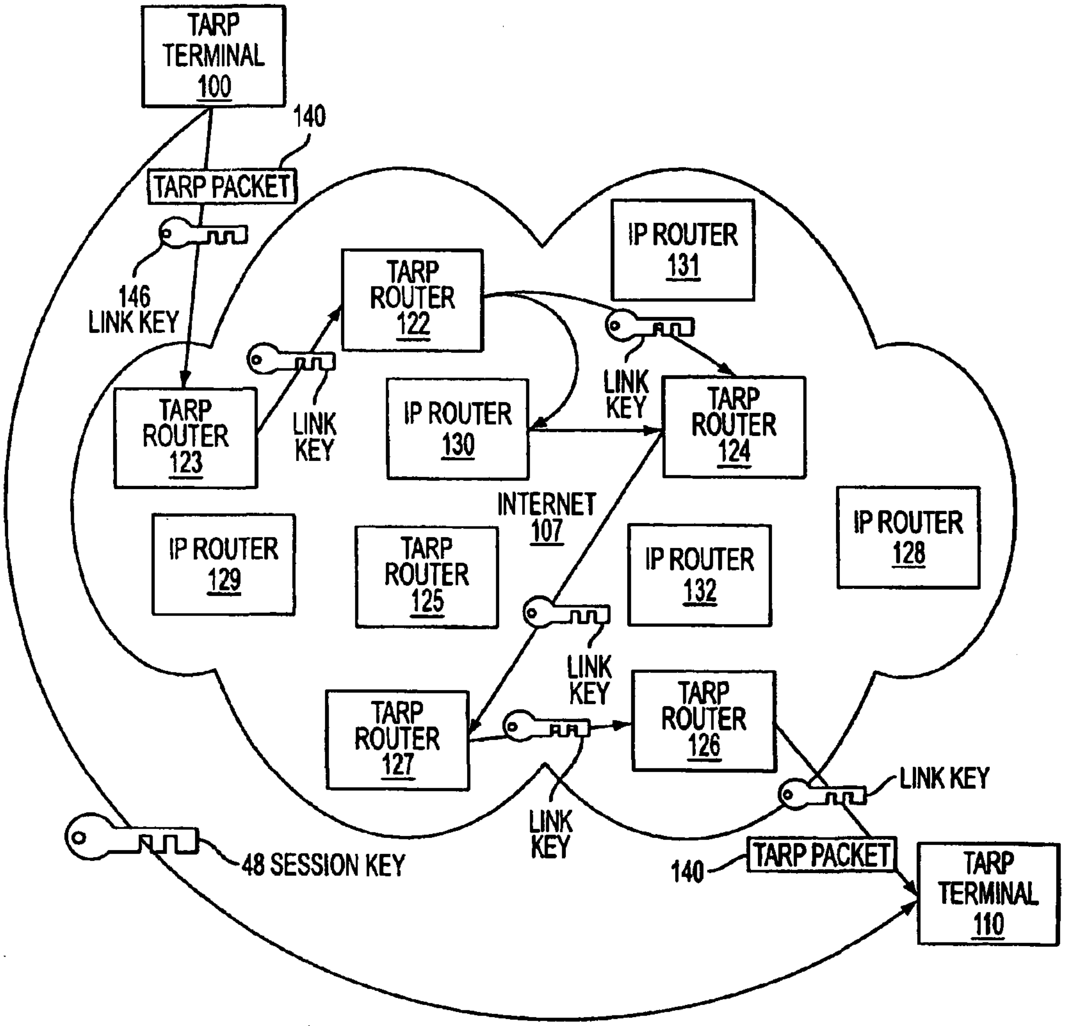

TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
TARP ROUTER 124
INTERNET 107
IP ROUTER 128
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
LINK KEY
TARP ROUTER 126
TARP ROUTER 127
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP PACKET
TARP TERMINAL 110

FIG. 2

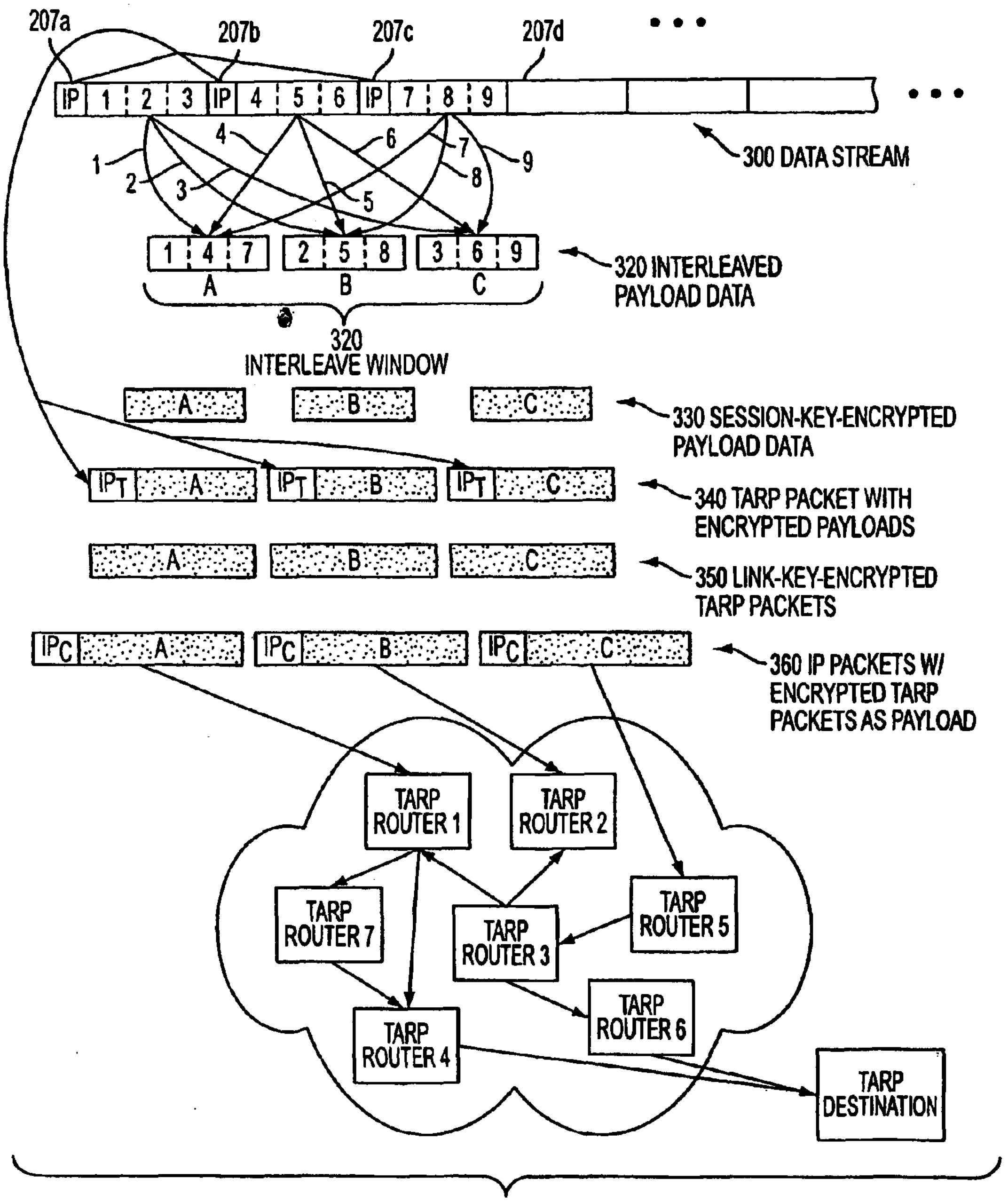

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
300 DATA STREAM
1
2
3
4
5
6
7
8
9
1 4 7
2 5 8
3 6 9
A
B
C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IPT A
IPT B
IPT C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
350 LINK-KEY-ENCRYPTED TARP PACKETS
IPC A
IPC B
IPC C
360 IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 6
TARP ROUTER 4
TARP DESTINATION

FIG. 3A

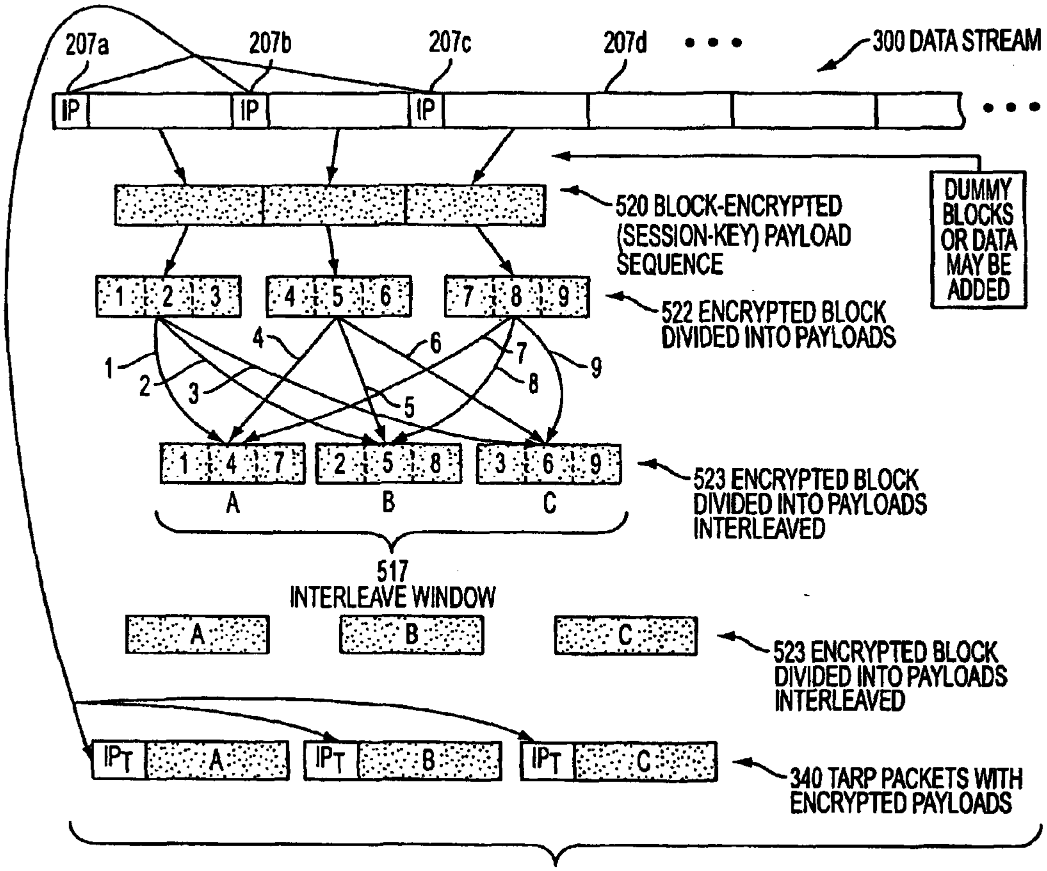

207a
207b
207c
207d • • •
300 DATA STREAM
IP
IP
IP
• • •
DUMMY BLOCKS OR DATA MAY BE ADDED
520 BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE
1 2 3
4 5 6
7 8 9
522 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS
1
2
3
4
5
6
7
8
9
1 4 7
2 5 8
3 6 9
A
B
C
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
517 INTERLEAVE WINDOW
A
B
C
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
IPT A
IPT B
IPT C
340 TARP PACKETS WITH ENCRYPTED PAYLOADS

FIG. 3B

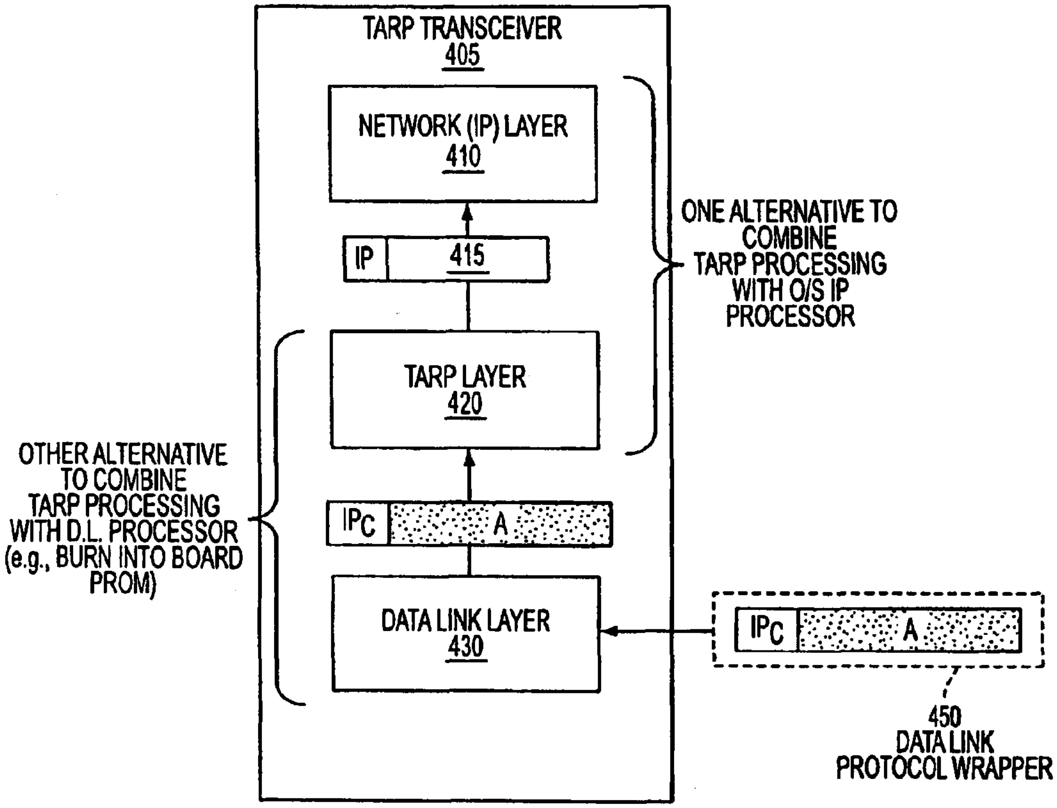

TARP TRANSCEIVER
405
NETWORK (IP) LAYER
410
IP
415
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
TARP LAYER
420
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (e.g., BURN INTO BOARD PROM)
IPc
A
DATA LINK LAYER
430
IPc
A
450
DATA LINK PROTOCOL WRAPPER

FIG. 4

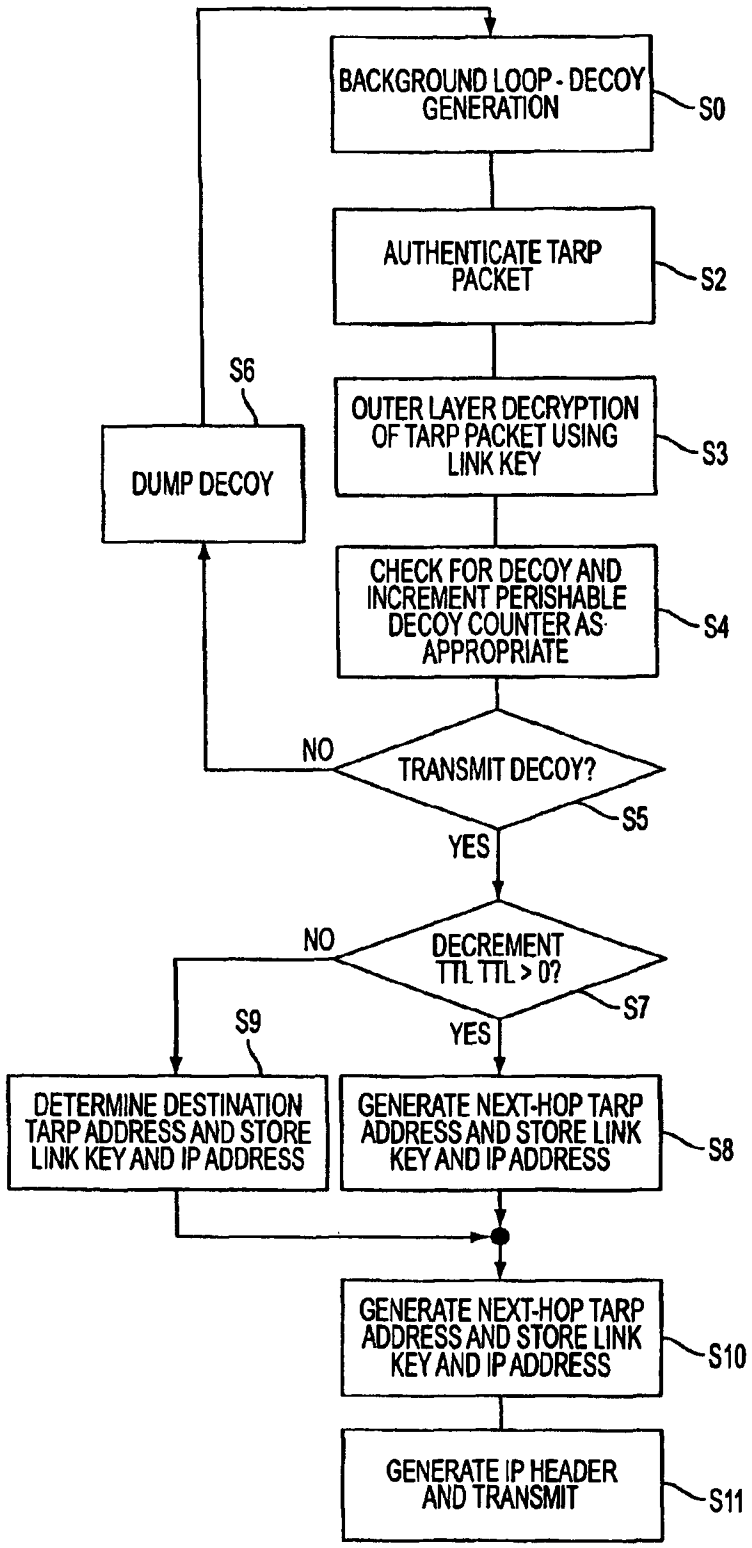

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
S6
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
DUMP DECOY
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
NO
TRANSMIT DECOY?
S5
YES
NO
DECREMENT TTL TTL > 0?
S7
S9
YES
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE IP HEADER AND TRANSMIT
S11

FIG. 5

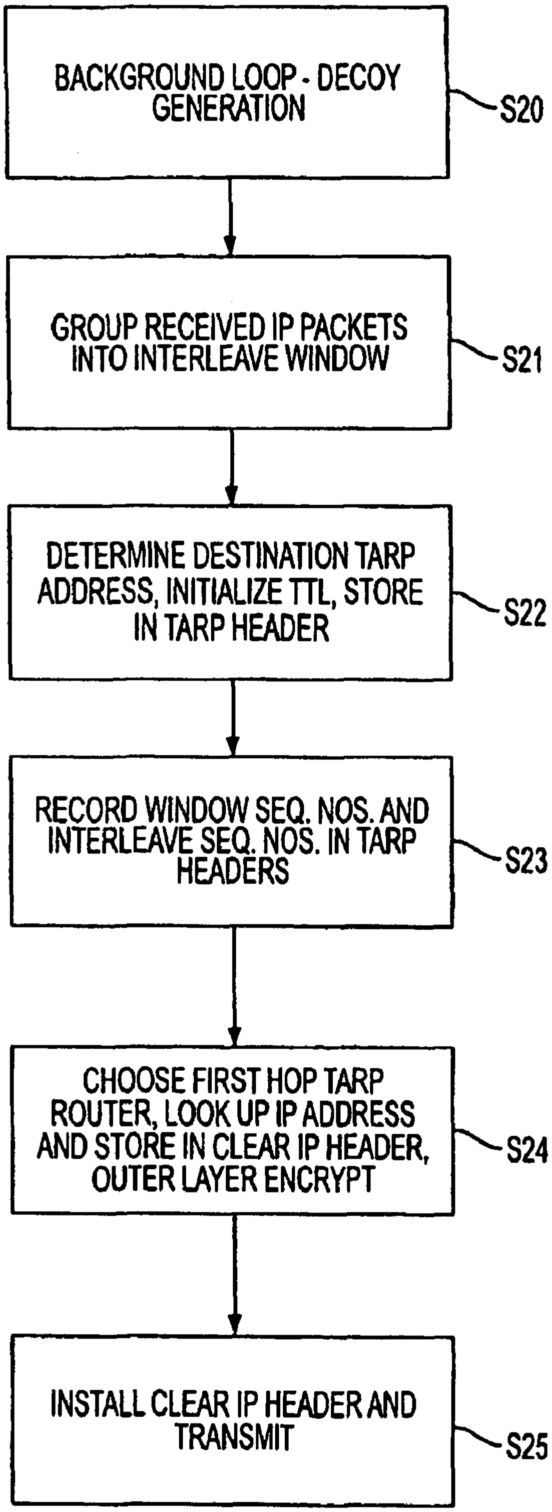

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

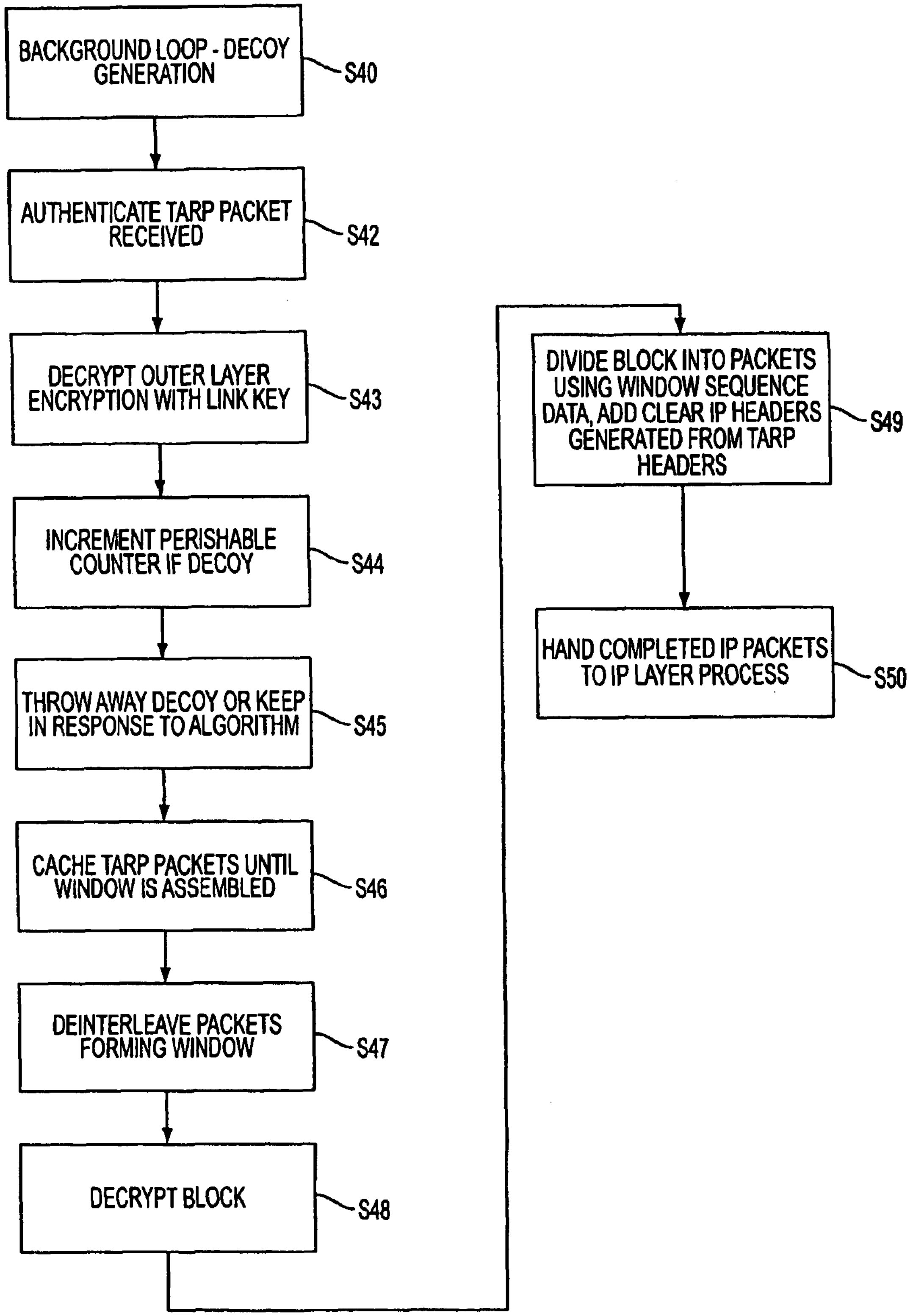

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
S47
DECRYPT BLOCK
S48
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S49
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS
S50

FIG. 7

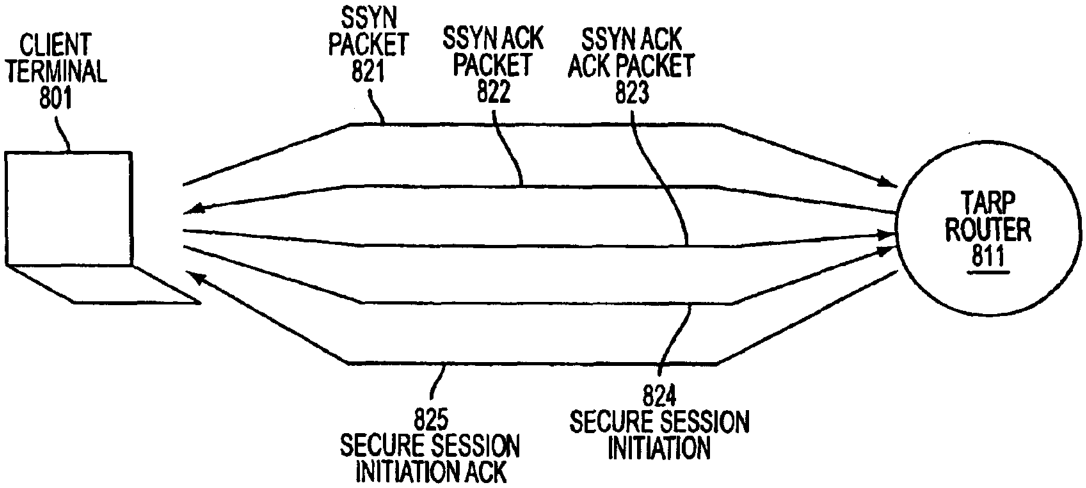
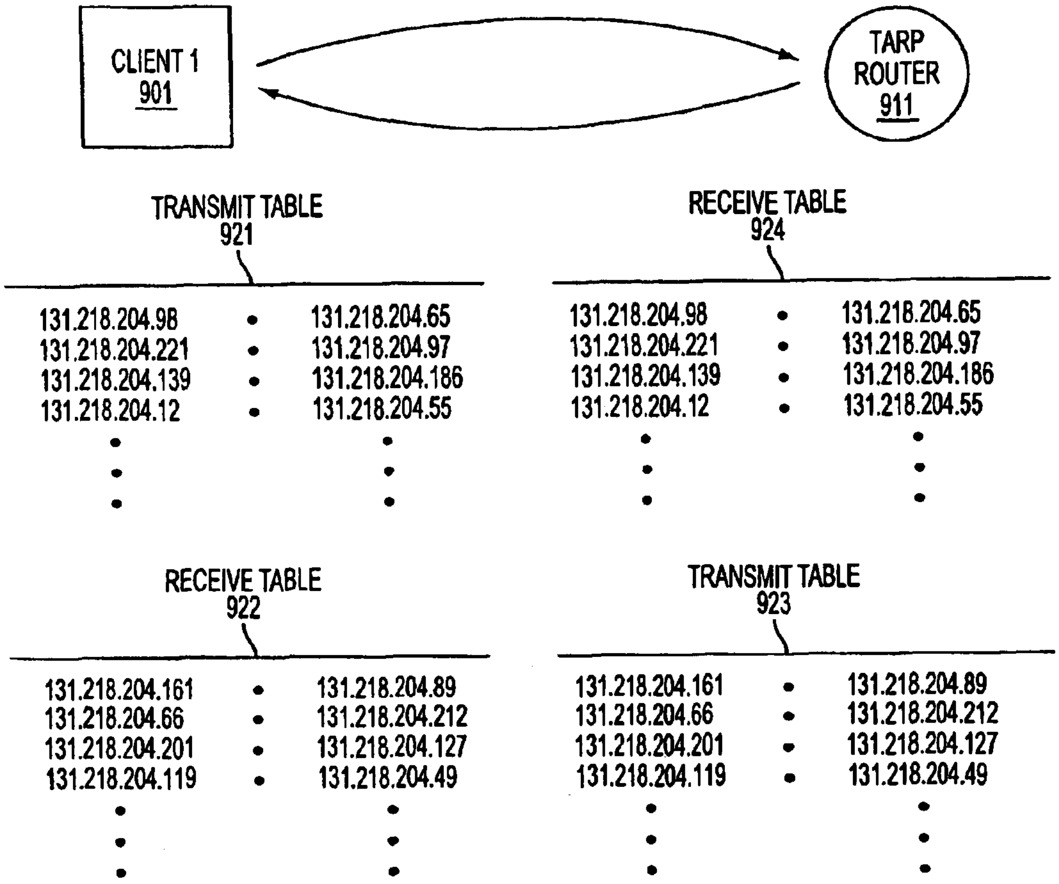

CLIENT TERMINAL 801
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
TARP ROUTER 811
825 SECURE SESSION INITIATION ACK
824 SECURE SESSION INITIATION

FIG. 8



TRANSMIT TABLE 921

131.218.204.98	•	131.218.204.65
131.218.204.221	•	131.218.204.97
131.218.204.139	•	131.218.204.186
131.218.204.12	•	131.218.204.55
•		•
•		•
•		•

RECEIVE TABLE 924

131.218.204.98	•	131.218.204.65
131.218.204.221	•	131.218.204.97
131.218.204.139	•	131.218.204.186
131.218.204.12	•	131.218.204.55
•		•
•		•
•		•

RECEIVE TABLE 922

131.218.204.161	•	131.218.204.89
131.218.204.66	•	131.218.204.212
131.218.204.201	•	131.218.204.127
131.218.204.119	•	131.218.204.49
•		•
•		•
•		•

TRANSMIT TABLE 923

131.218.204.161	•	131.218.204.89
131.218.204.66	•	131.218.204.212
131.218.204.201	•	131.218.204.127
131.218.204.119	•	131.218.204.49
•		•
•		•
•		•

FIG. 9

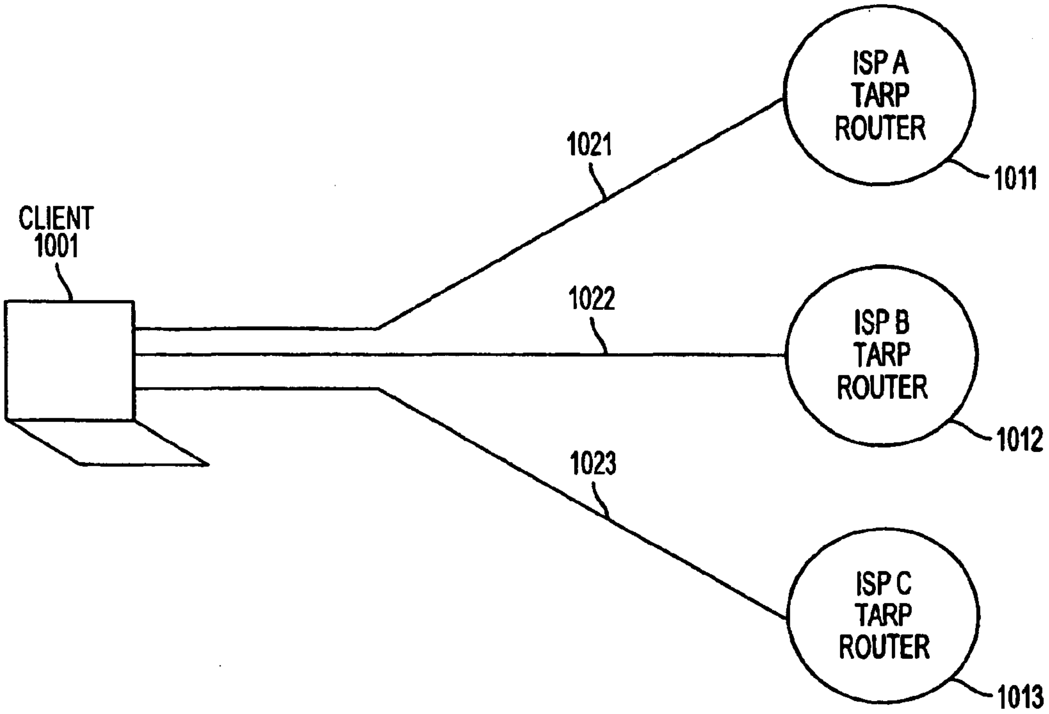

ISP A
TARP
ROUTER
1011
1021
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

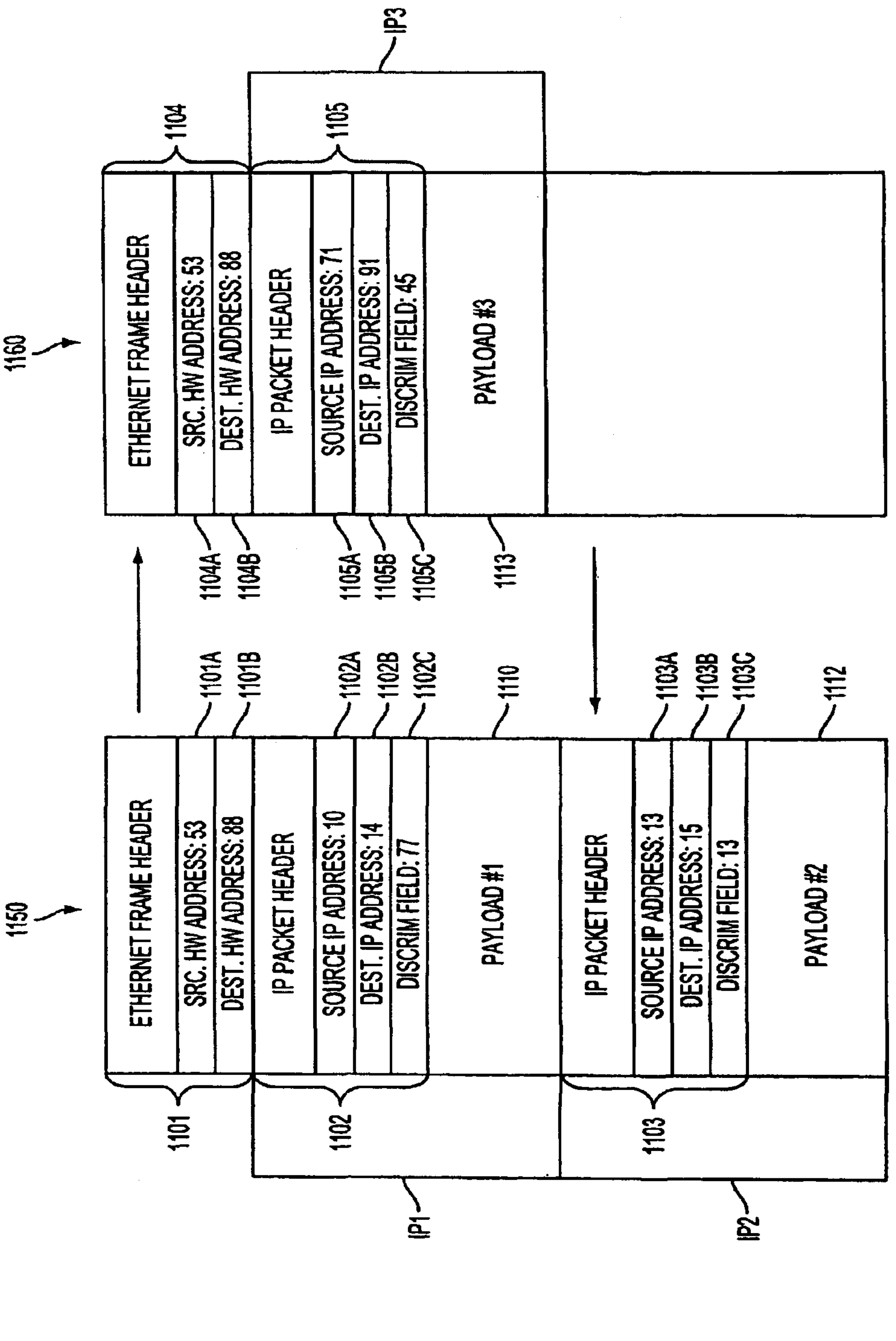
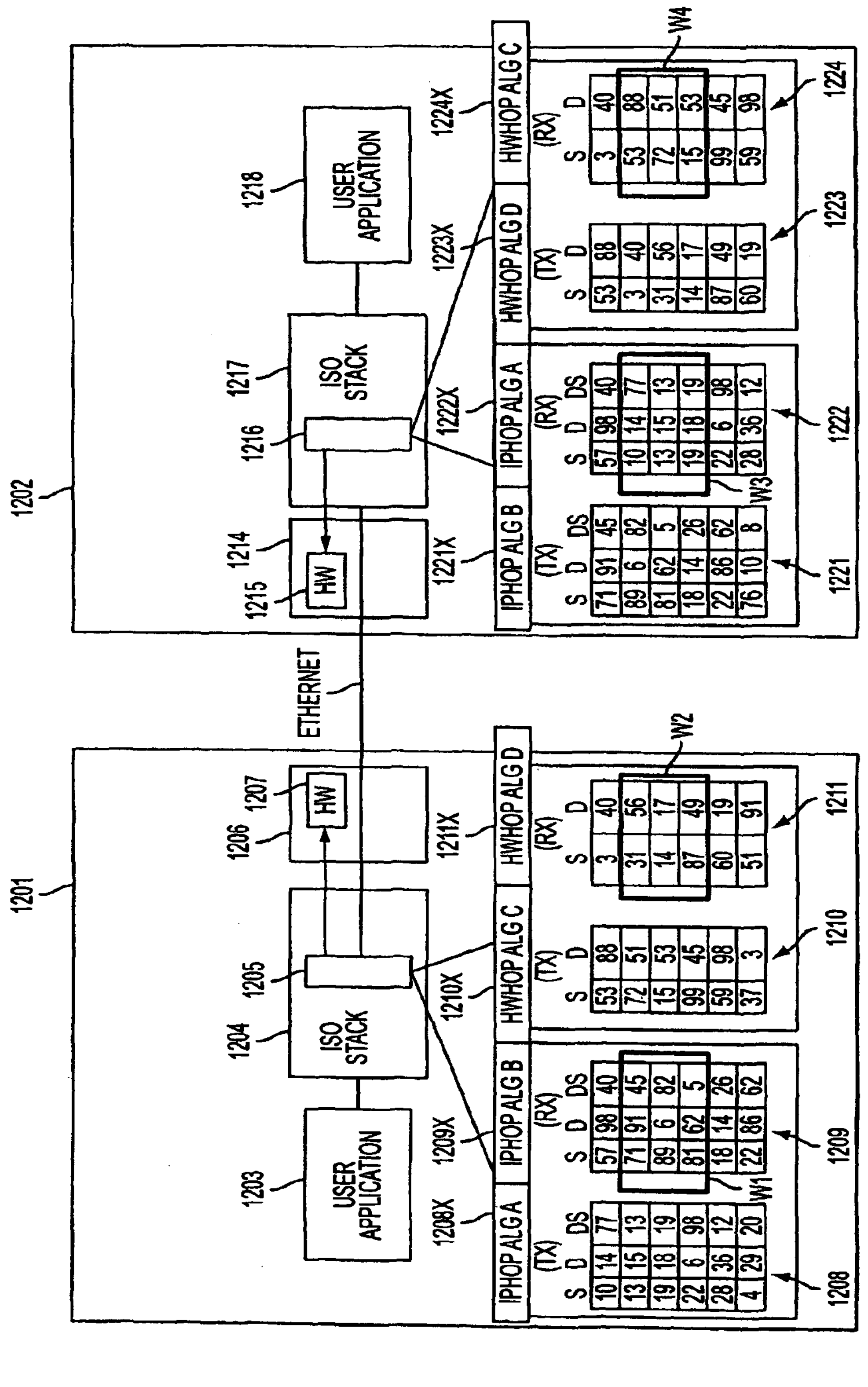

1150
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
1101
1102
1103
IP1
IP2
1101A
1101B
1102A
1102B
1102C
1110
1103A
1103B
1103C
1112
1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 71
DEST. IP ADDRESS: 91
DISCRIM FIELD: 45
PAYLOAD #3
1104
1105
IP3
1104A
1104B
1105A
1105B
1105C
1113

FIG. 11



1208 IPHOP ALG A (TX)

S	D	DS
10	14	77
13	15	13
19	18	19
22	6	98
28	36	12
4	29	20

1209 IPHOP ALG B (RX)

S	D	DS
57	98	40
71	91	45
89	6	82
81	62	5
18	14	26
22	86	62

1210 HWHOP ALG C (TX)

S	D
53	88
72	51
15	53
99	45
59	98
37	3

1211 HWHOP ALG D (RX)

S	D
3	40
31	56
14	17
87	49
60	19
51	91

1221 IPHOP ALG B (TX)

S	D	DS
71	91	45
89	6	82
81	62	5
18	14	26
22	86	62
76	10	8

1222 IPHOP ALG A (RX)

S	D	DS
57	98	40
10	14	77
13	15	13
19	18	19
22	6	98
28	36	12

1223 HWHOP ALG D (TX)

S	D
53	88
3	40
31	56
14	17
87	49
60	19

1224 HWHOP ALG C (RX)

S	D
3	40
53	88
72	51
15	53
99	45
59	98

FIG. 12A

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

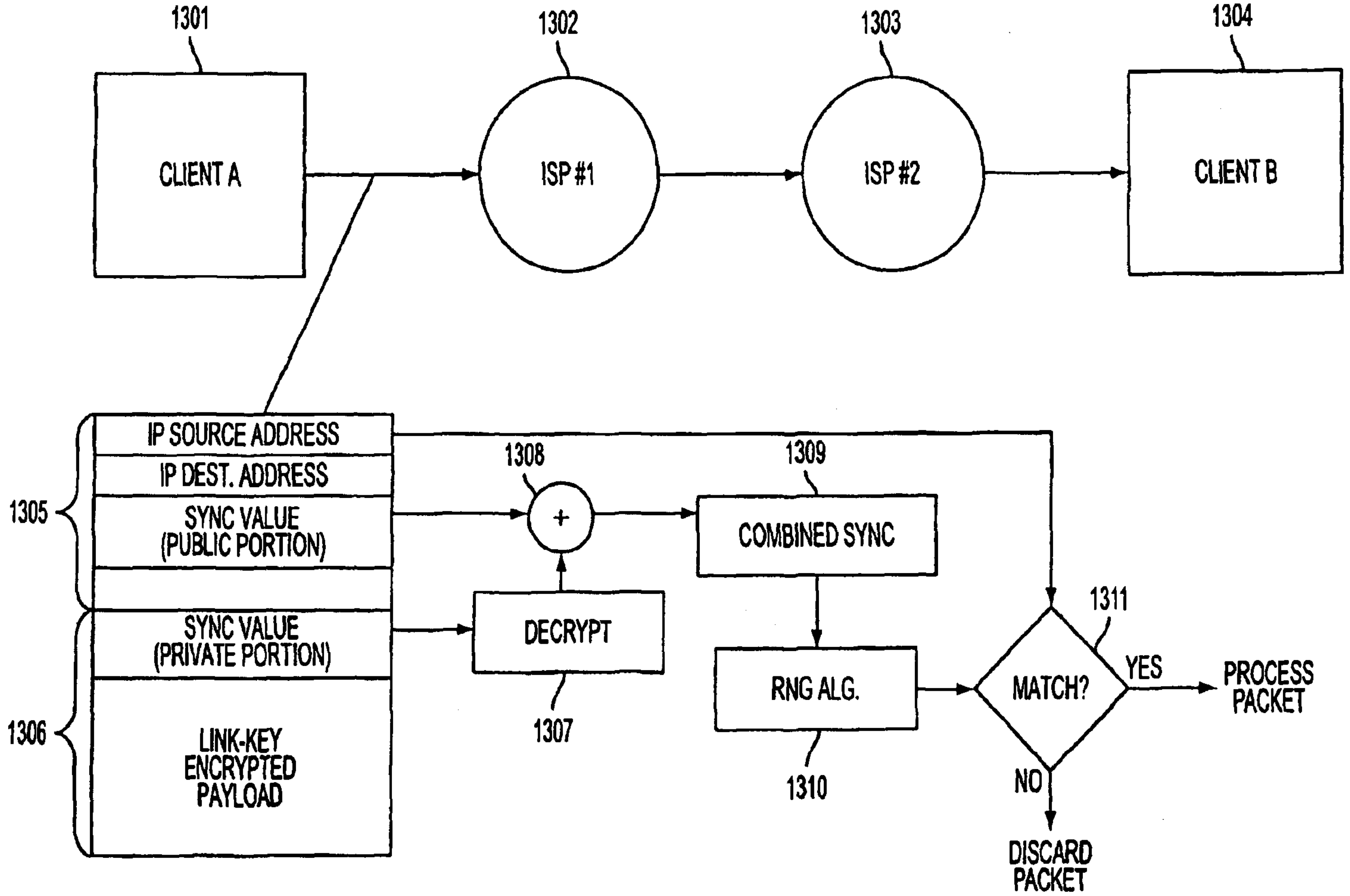

1301
CLIENT A
1302
ISP #1
1303
ISP #2
1304
CLIENT B
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE
(PUBLIC PORTION)
SYNC VALUE
(PRIVATE PORTION)
LINK-KEY
ENCRYPTED
PAYLOAD
1305
1306
1308
+
1309
COMBINED SYNC
DECRYPT
1307
RNG ALG.
1310
1311
MATCH?
YES
PROCESS
PACKET
NO
DISCARD
PACKET

FIG. 13

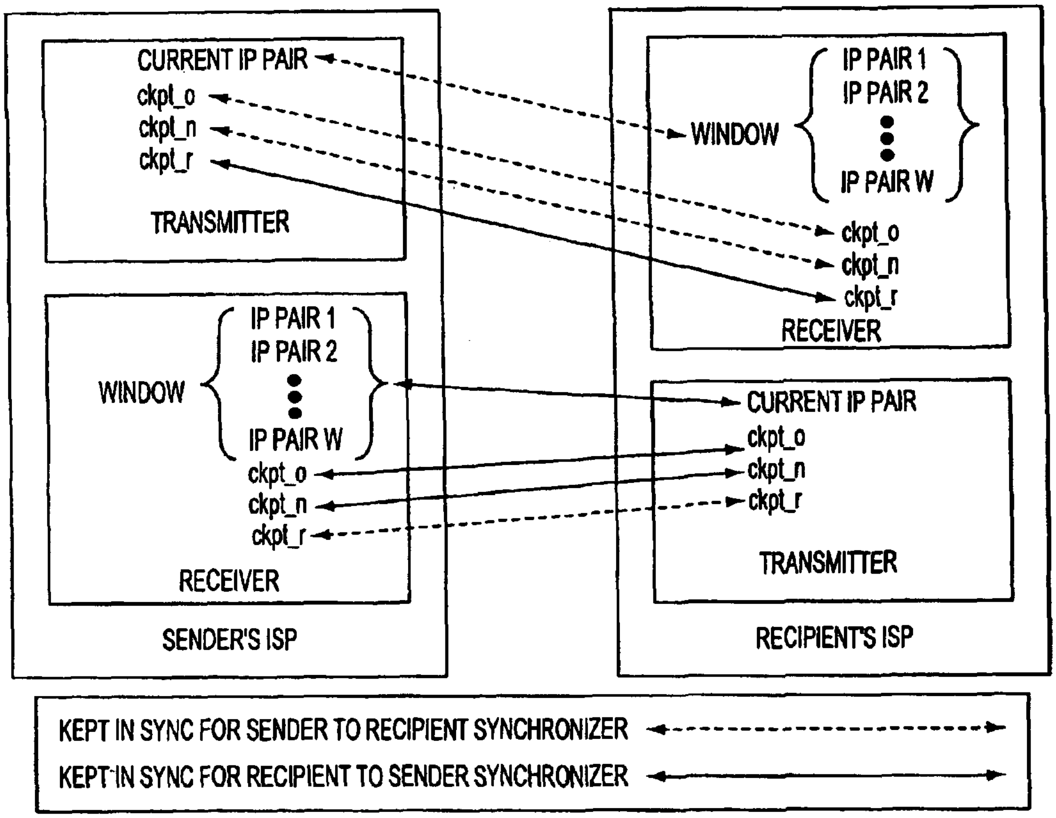

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
SENDER'S ISP
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

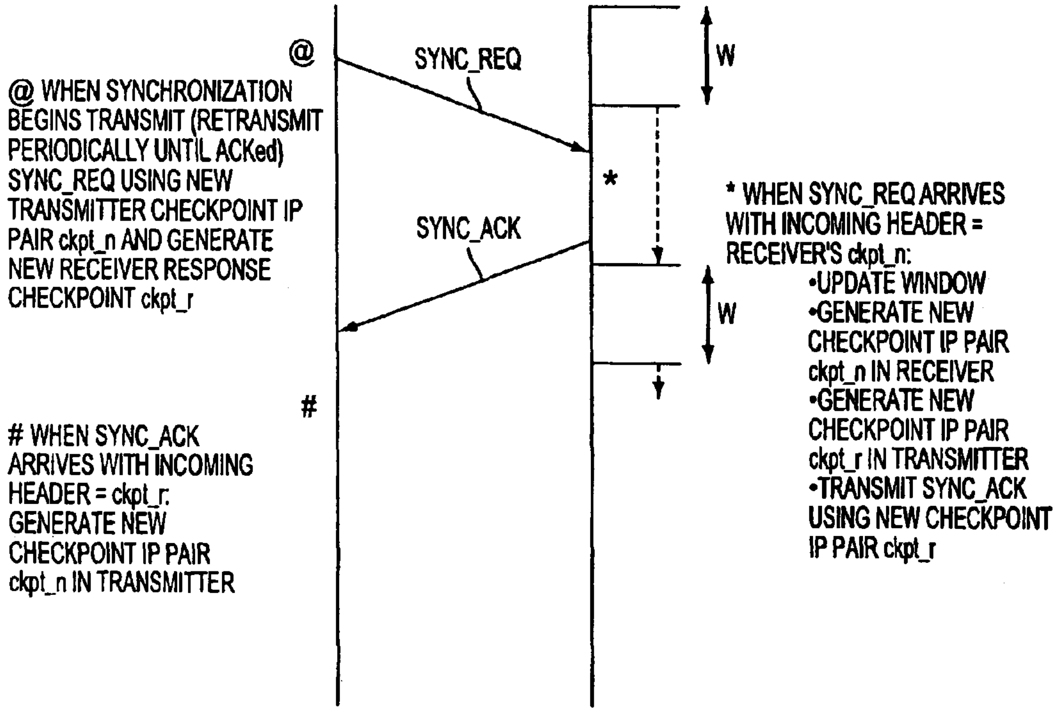

@
SYNC_REQ
W
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
*
SYNC_ACK
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
•GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
•TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r
W
#
# WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER

FIG. 15

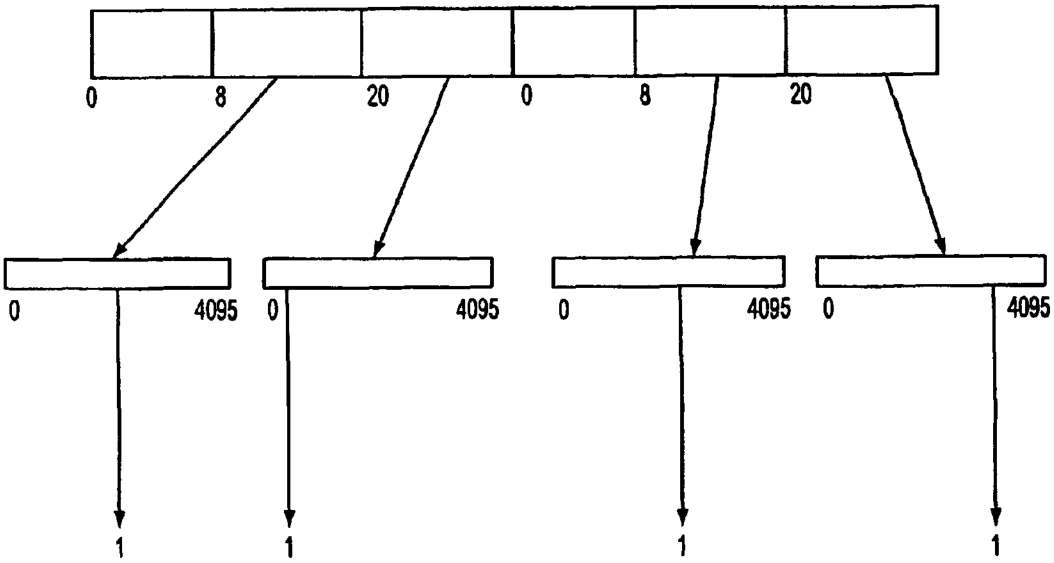


FIG. 16

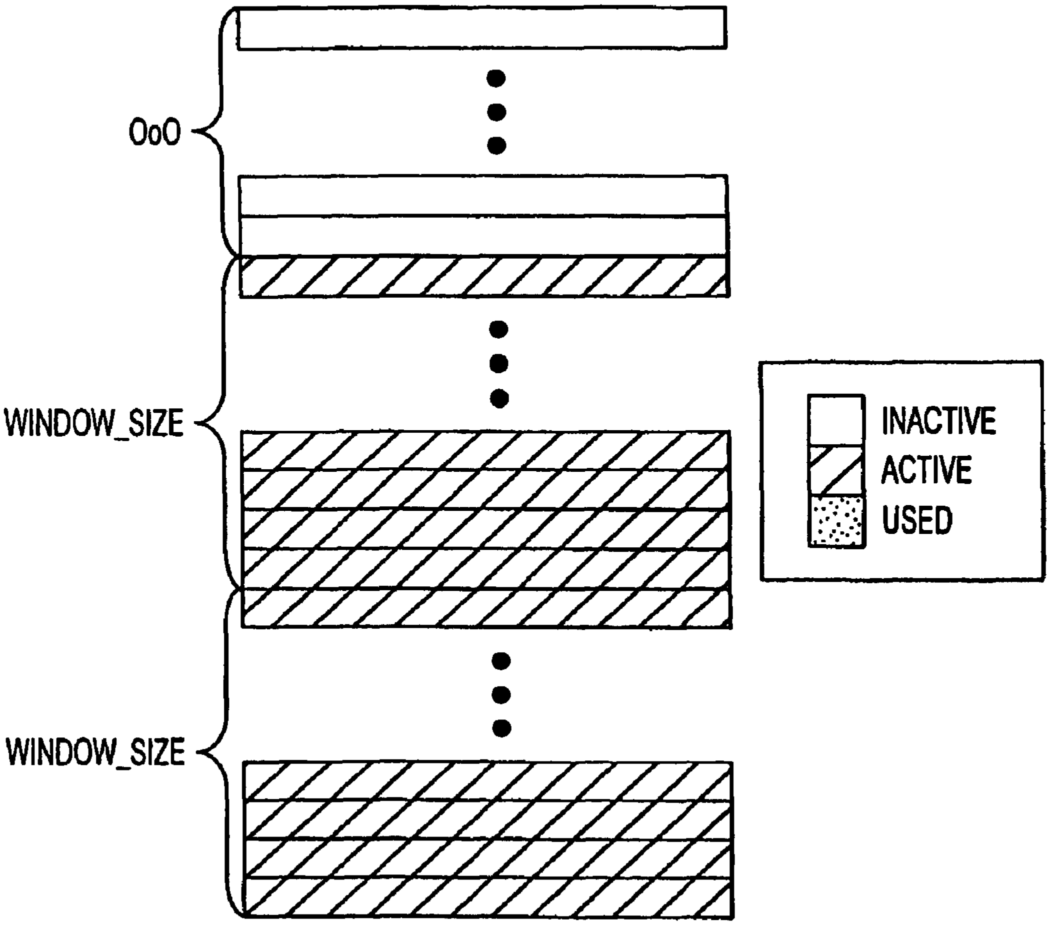


FIG. 17

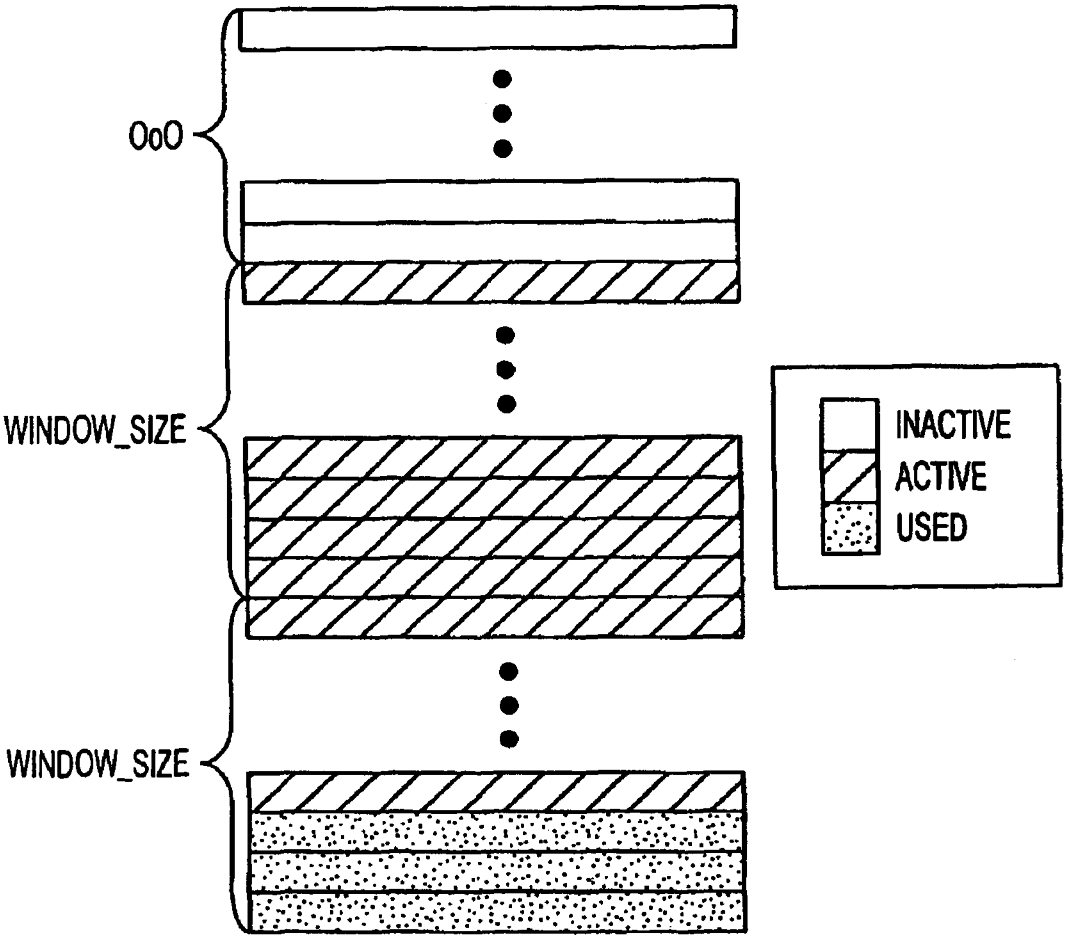


FIG. 18

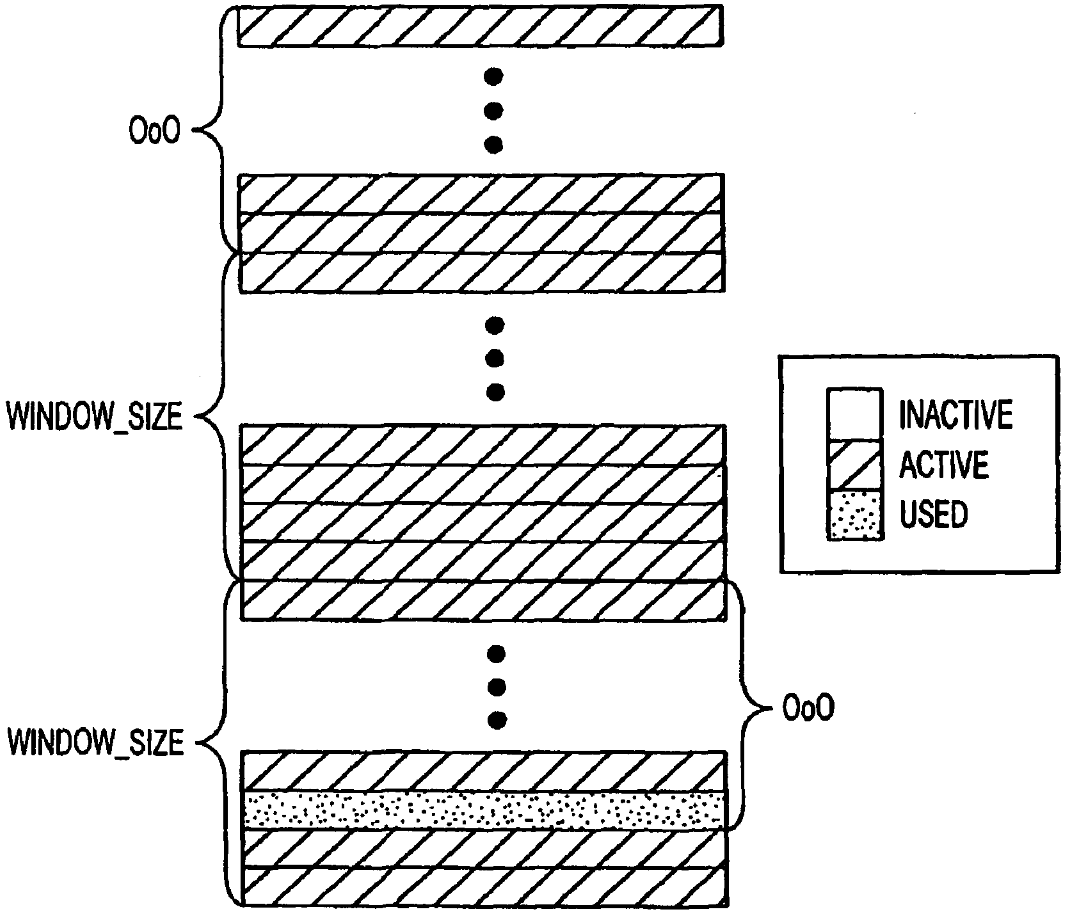


FIG. 19

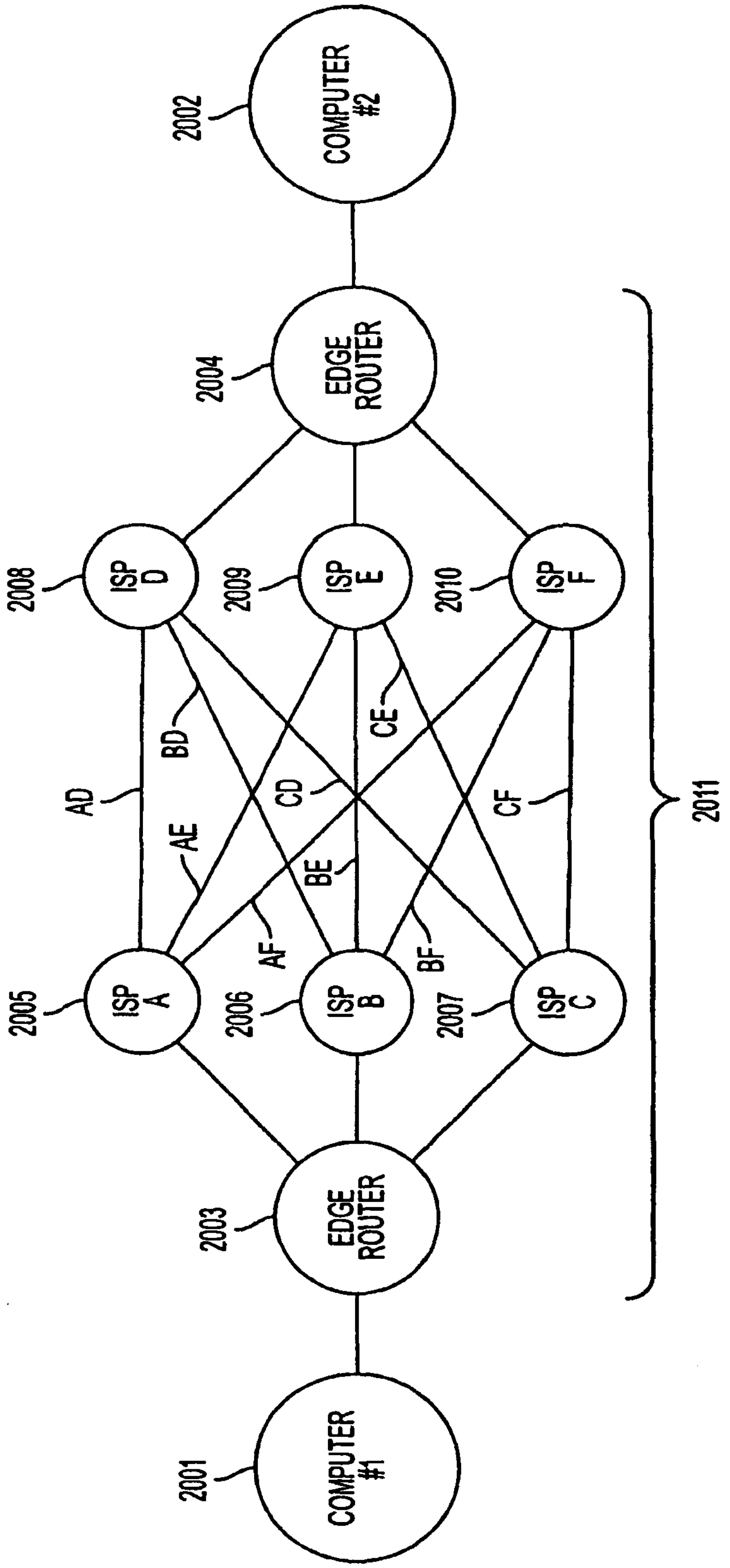

2001
COMPUTER #1
2003
EDGE ROUTER
2005
ISP A
2006
ISP B
2007
ISP C
AD
AE
AF
BD
BE
BF
CD
CE
CF
2008
ISP D
2009
ISP E
2010
ISP F
2004
EDGE ROUTER
2002
COMPUTER #2
2011

FIG. 20

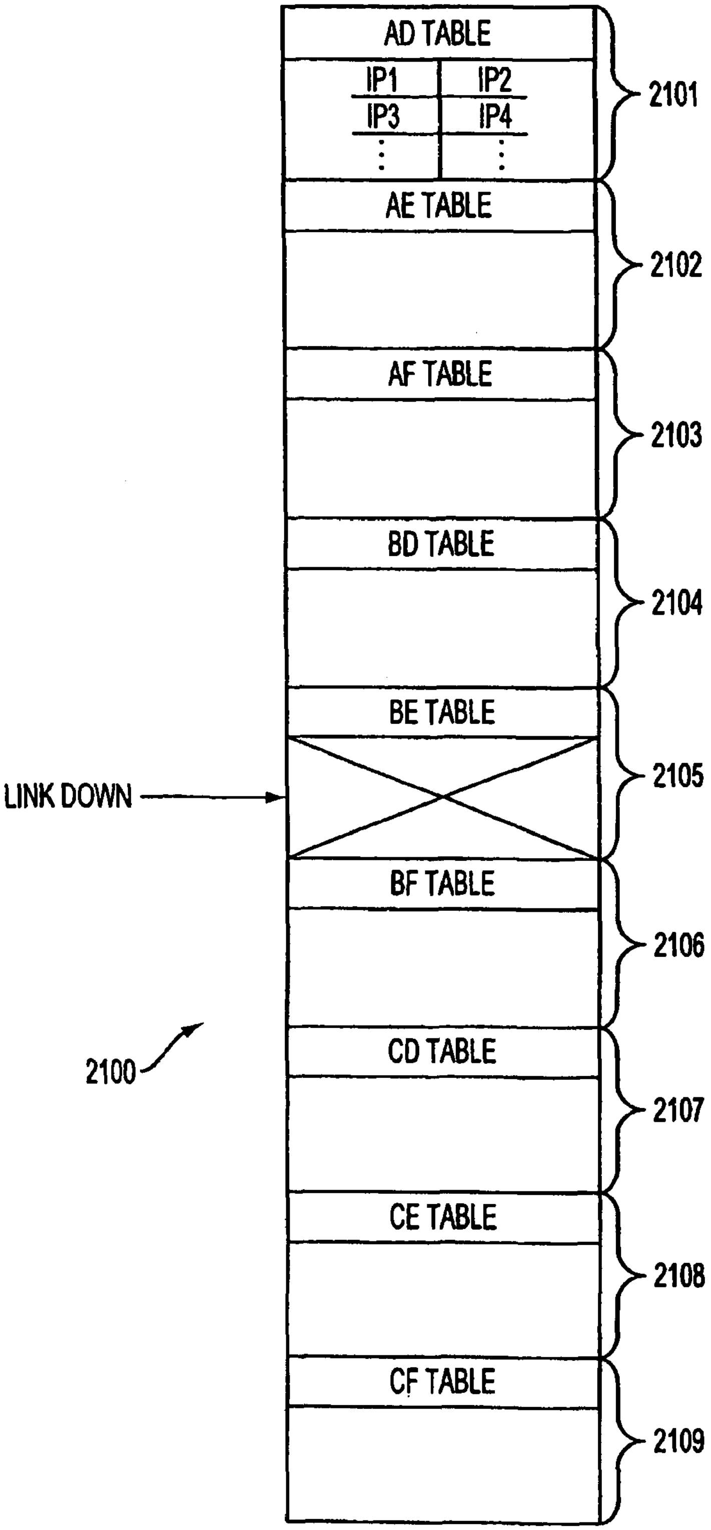

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
LINK DOWN
2105
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21

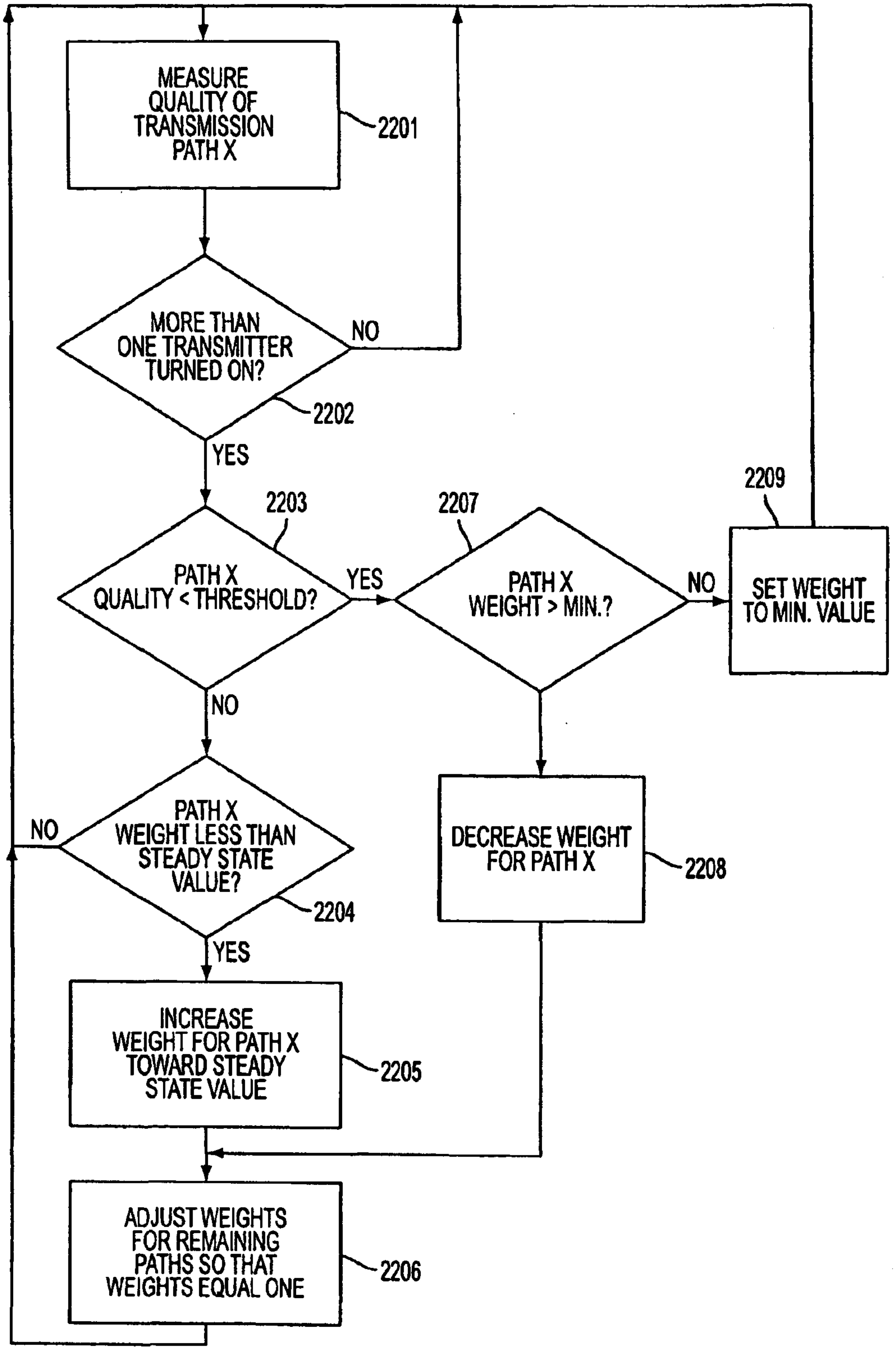

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
NO
2202
YES
2203
PATH X QUALITY < THRESHOLD?
YES
2207
PATH X WEIGHT > MIN.?
NO
2209
SET WEIGHT TO MIN. VALUE
NO
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
2204
YES
DECREASE WEIGHT FOR PATH X
2208
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2206

FIG. 22A

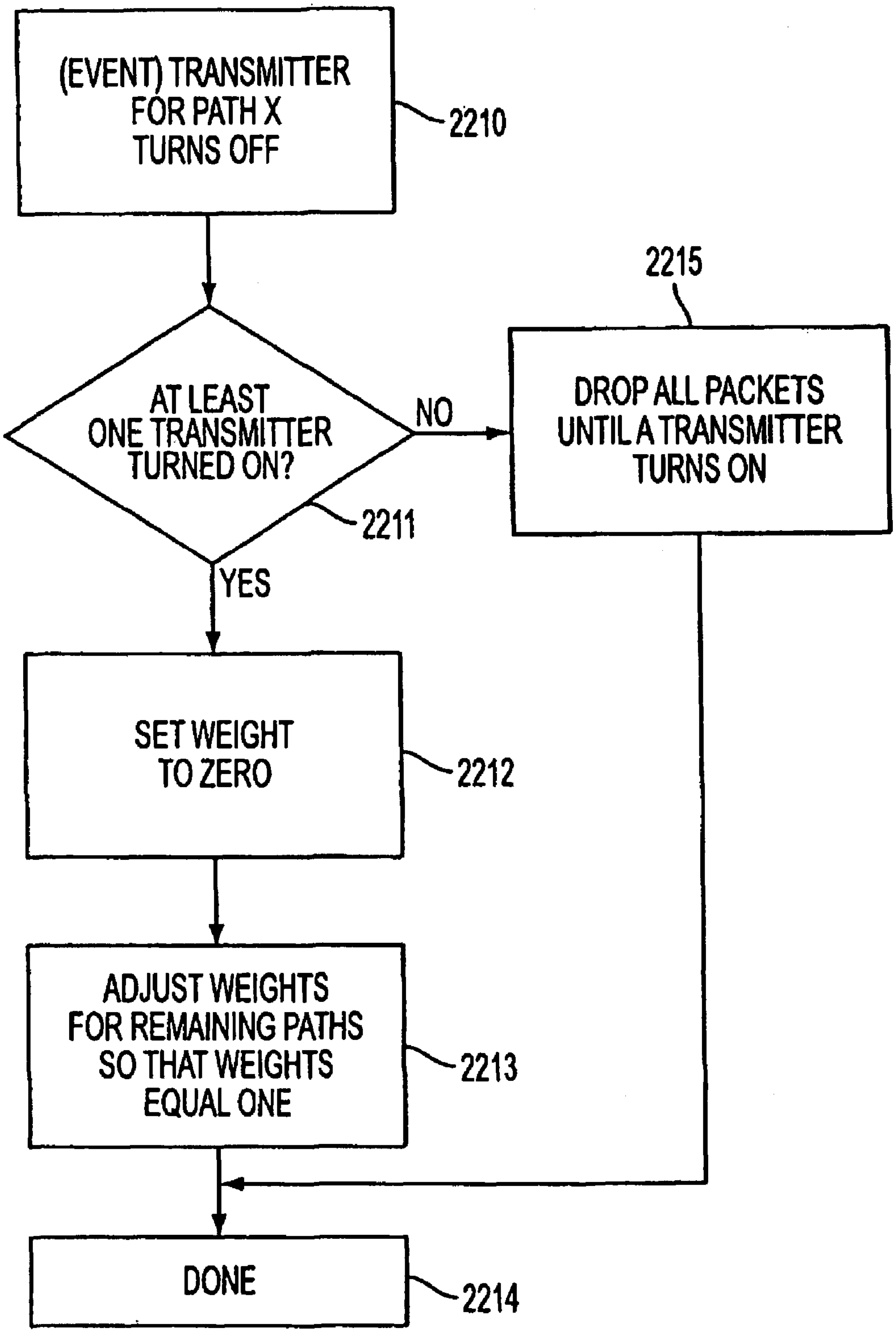

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
AT LEAST ONE TRANSMITTER TURNED ON?
2211
NO
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
2215
YES
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

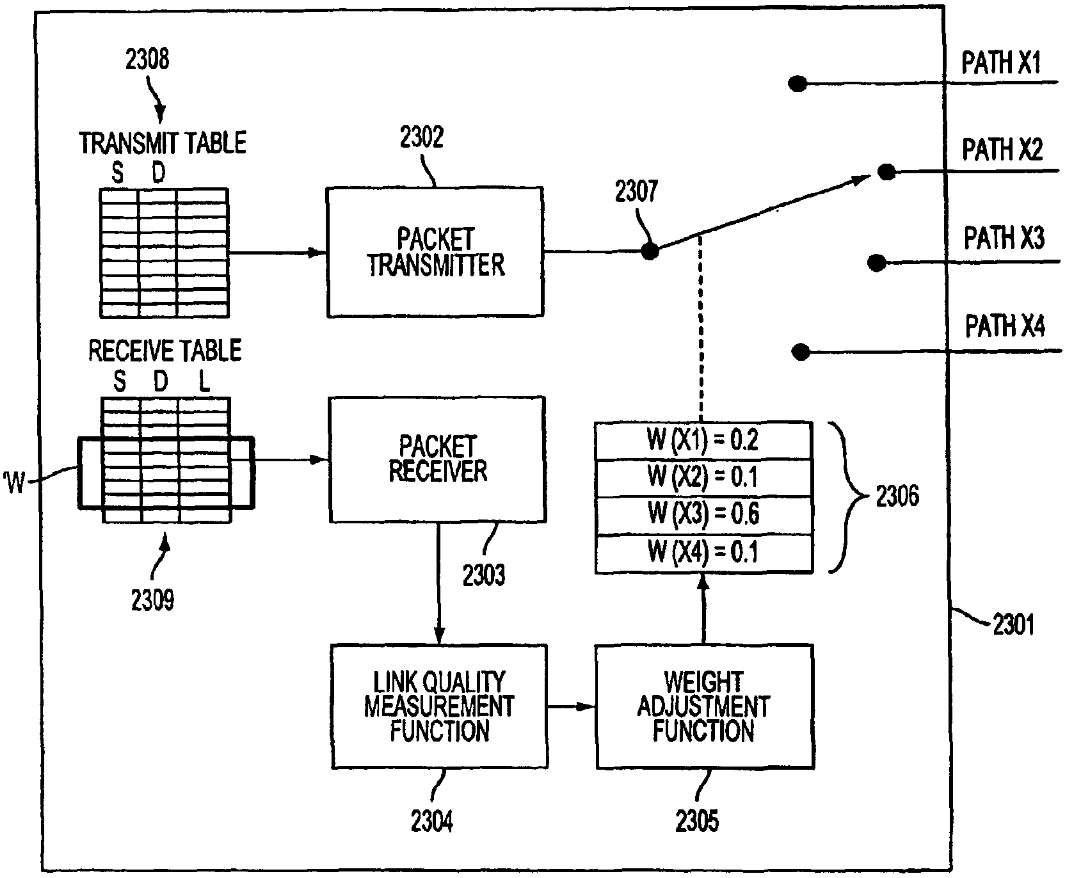

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

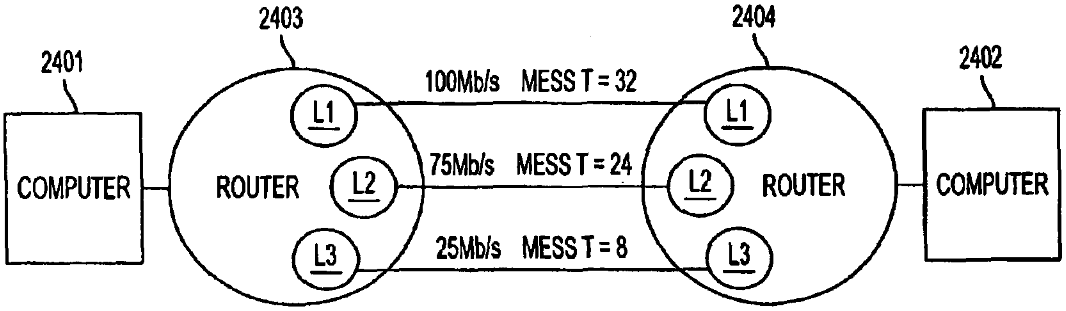

2401
COMPUTER
2403
ROUTER
L1
L2
L3
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
2404
L1
L2
L3
ROUTER
2402
COMPUTER

FIG. 24

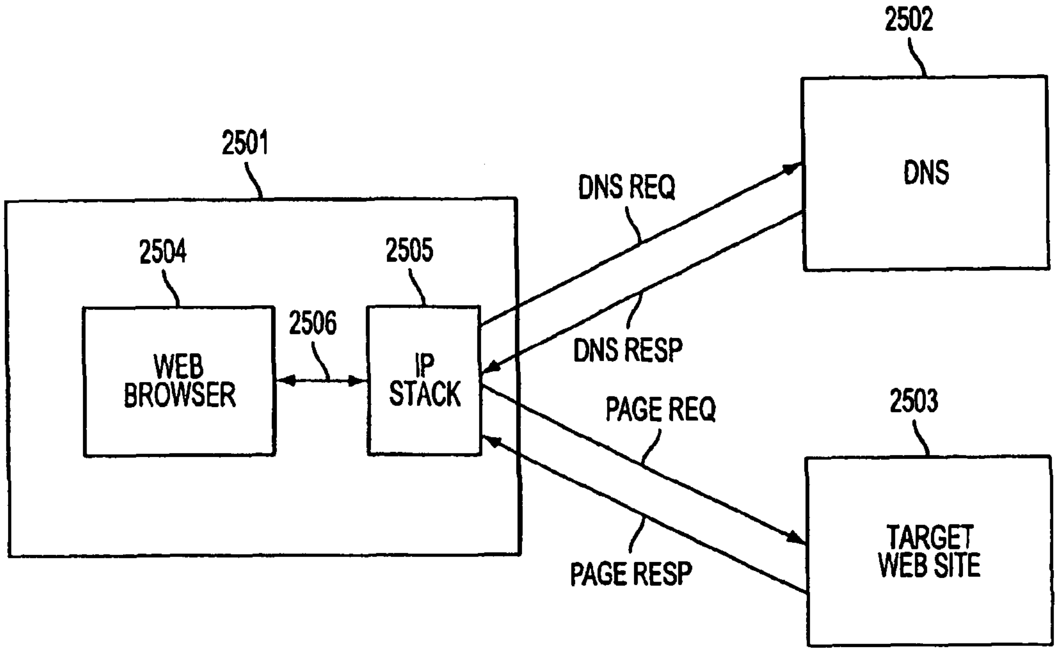


FIG. 25
(PRIOR ART)

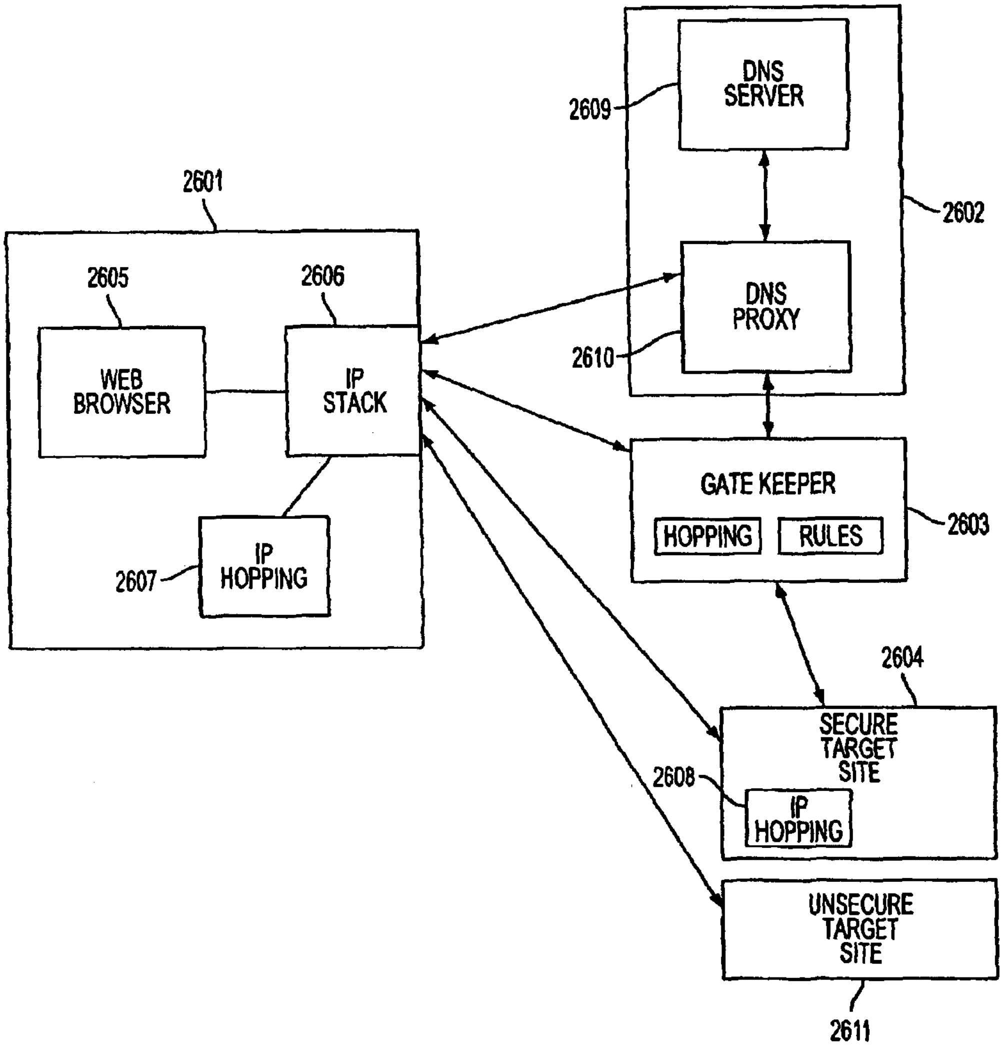

2601
2605
2606
WEB BROWSER
IP STACK
2607
IP HOPPING
2609
DNS SERVER
2602
2610
DNS PROXY
GATE KEEPER
HOPPING
RULES
2603
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

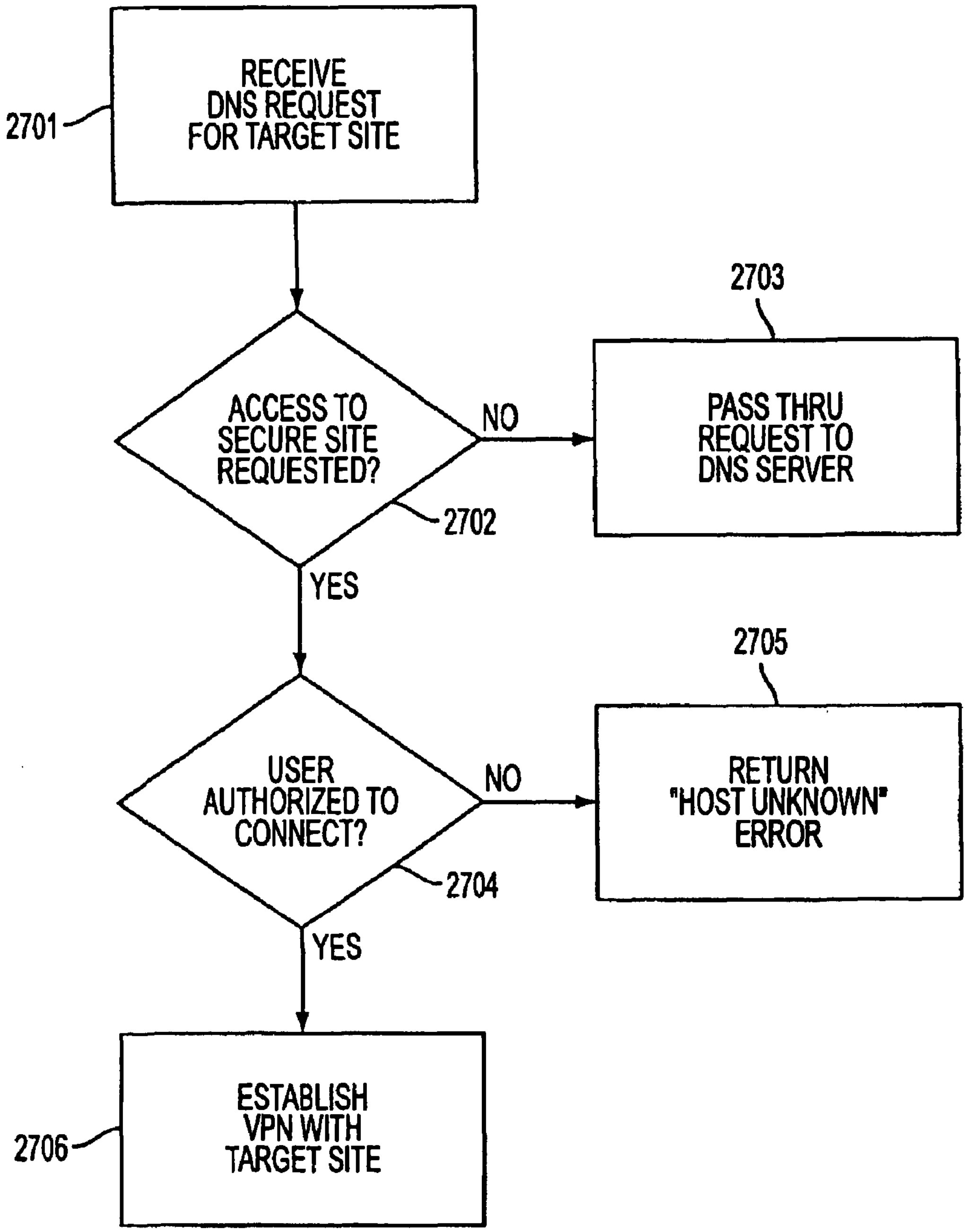

RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
2702
NO
PASS THRU REQUEST TO DNS SERVER
2703
YES
USER AUTHORIZED TO CONNECT?
2704
NO
RETURN "HOST UNKNOWN" ERROR
2705
YES
ESTABLISH VPN WITH TARGET SITE
2706

FIG. 27

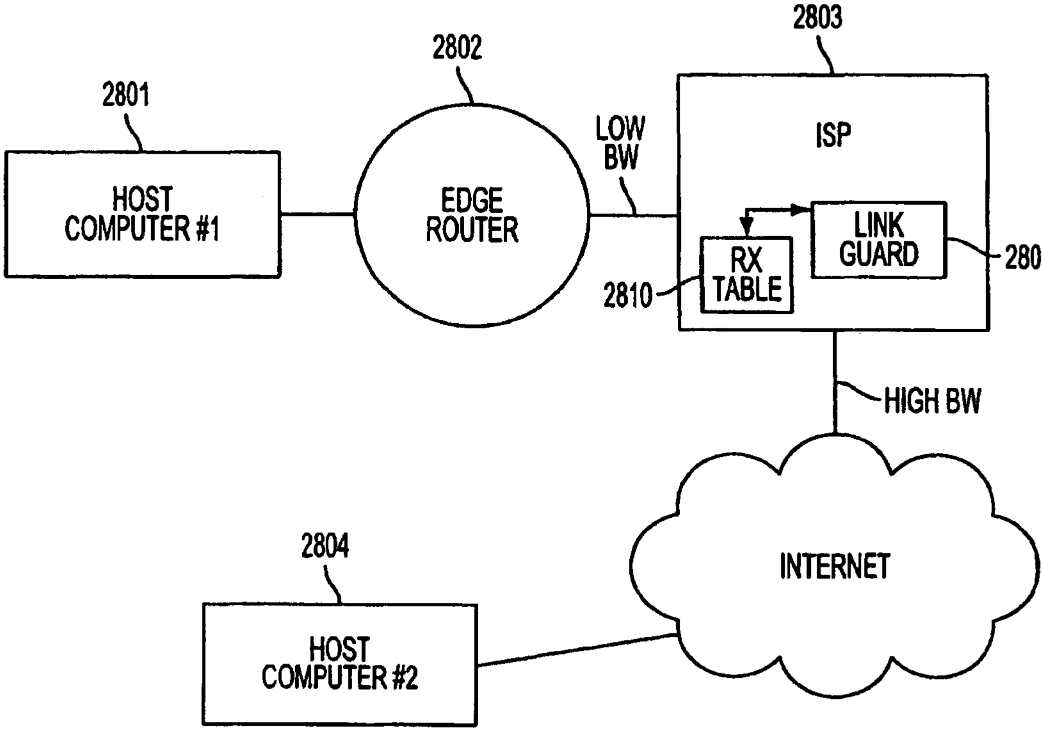

2803
2802
2801
LOW BW
ISP
HOST COMPUTER #1
EDGE ROUTER
LINK GUARD
2805
RX TABLE
2810
HIGH BW
INTERNET
2804
HOST COMPUTER #2

FIG. 28

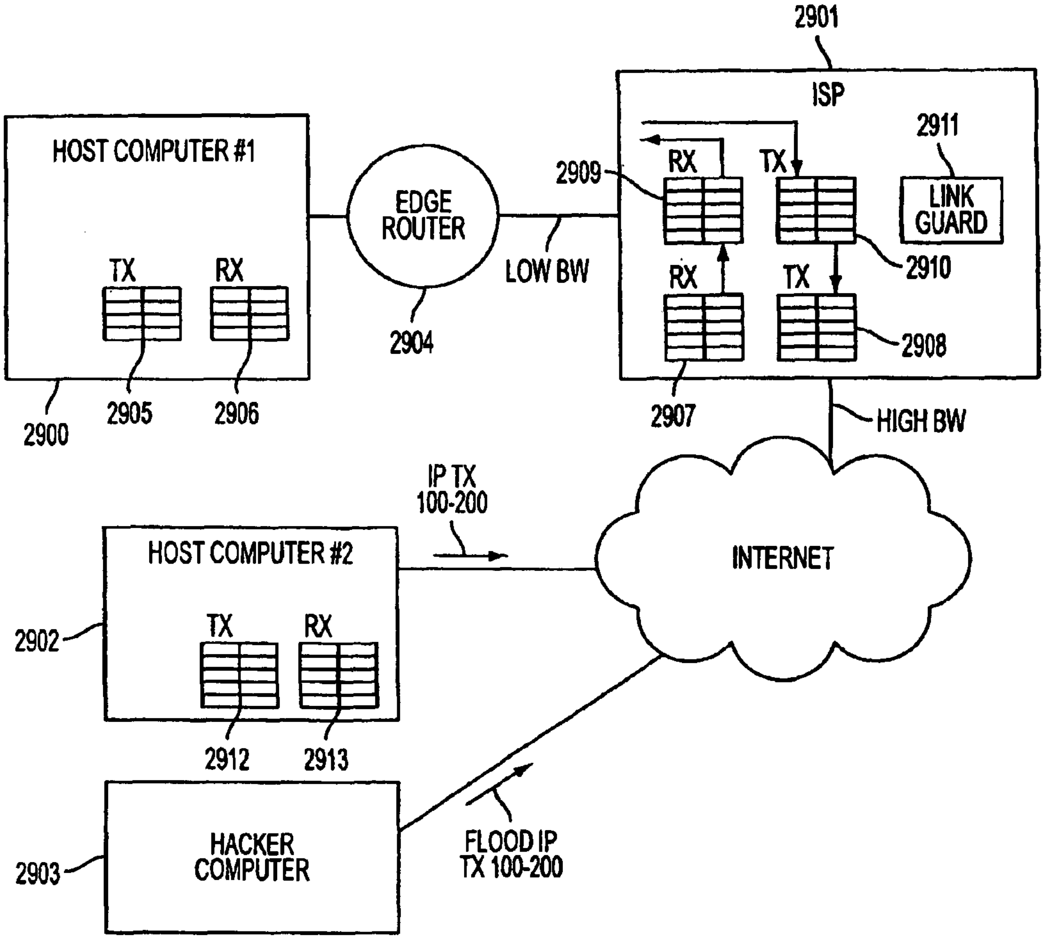

2901
ISP
2911
LINK GUARD
2909
RX
TX
2910
RX
TX
2908
2907
HOST COMPUTER #1
TX
RX
2900
2905
2906
EDGE ROUTER
2904
LOW BW
HIGH BW
INTERNET
IP TX 100-200
HOST COMPUTER #2
TX
RX
2902
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29

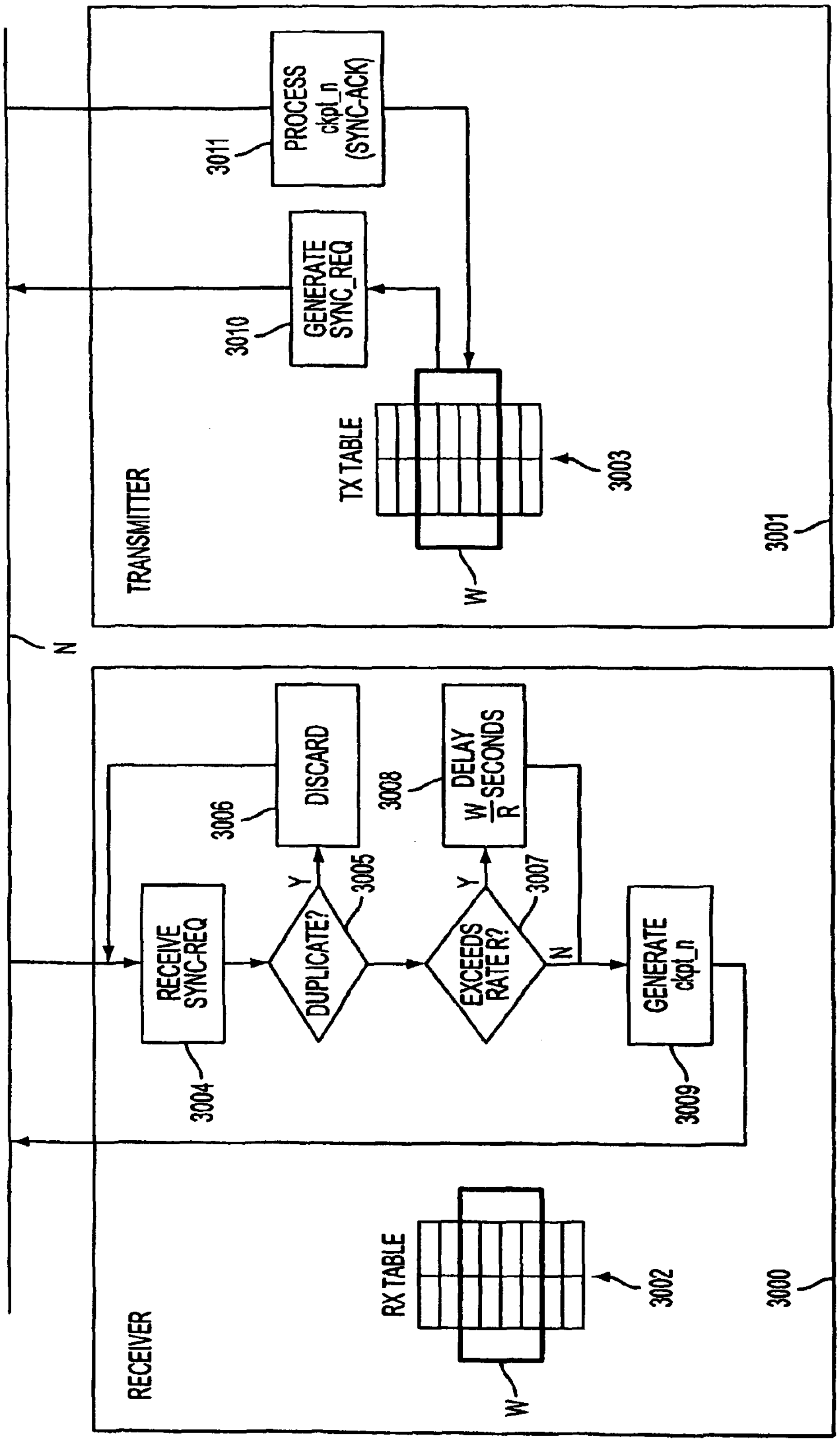

TRANSMITTER
3001
TX TABLE
3003
W
GENERATE SYNC_REQ
3010
PROCESS ckpt_n (SYNC-ACK)
3011
N
RECEIVER
3000
RX TABLE
3002
W
RECEIVE SYNC-REQ
3004
DUPLICATE?
3005
Y
DISCARD
3006
EXCEEDS RATE R?
3007
Y
N
DELAY $\frac{W}{R}$ SECONDS
3008
GENERATE ckpt_n
3009

FIG. 30

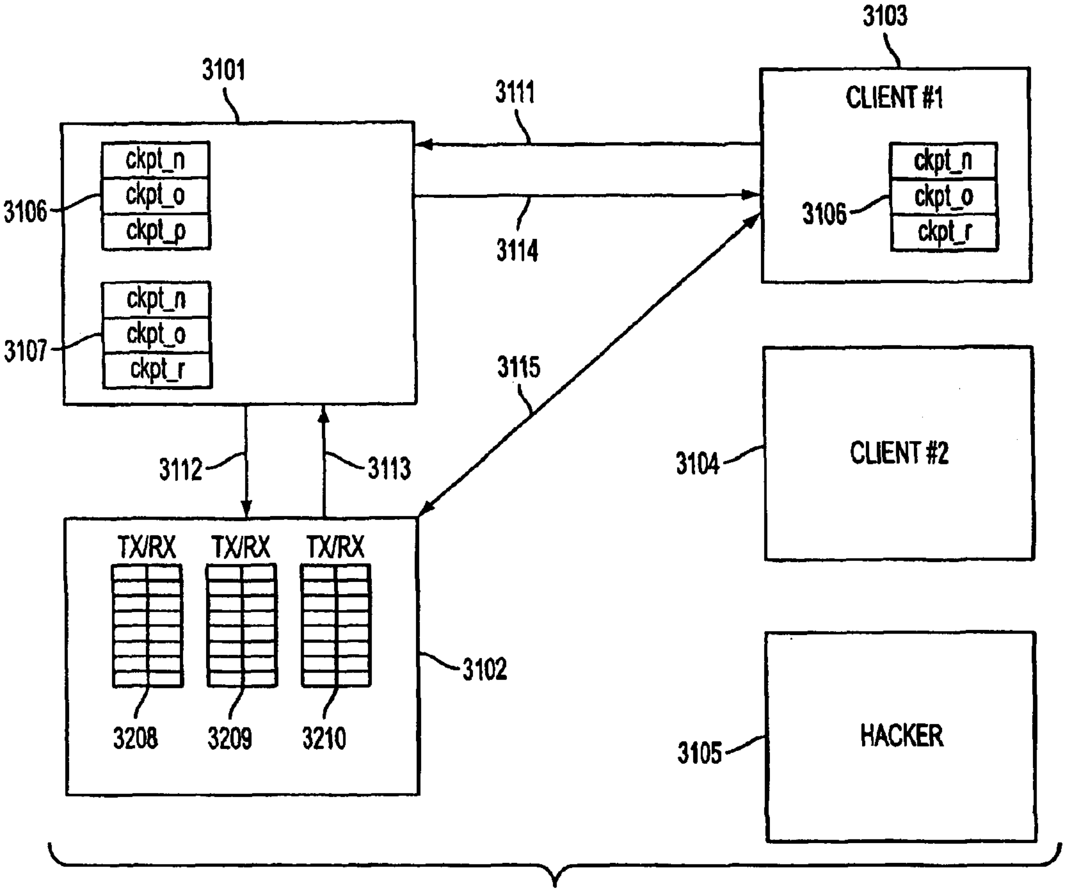

3101
3103
CLIENT #1
3111
3114
3106
ckpt_n
ckpt_o
ckpt_p
3107
ckpt_n
ckpt_o
ckpt_r
3106
ckpt_n
ckpt_o
ckpt_r
3115
3112
3113
CLIENT #2
3104
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
HACKER
3105

FIG. 31

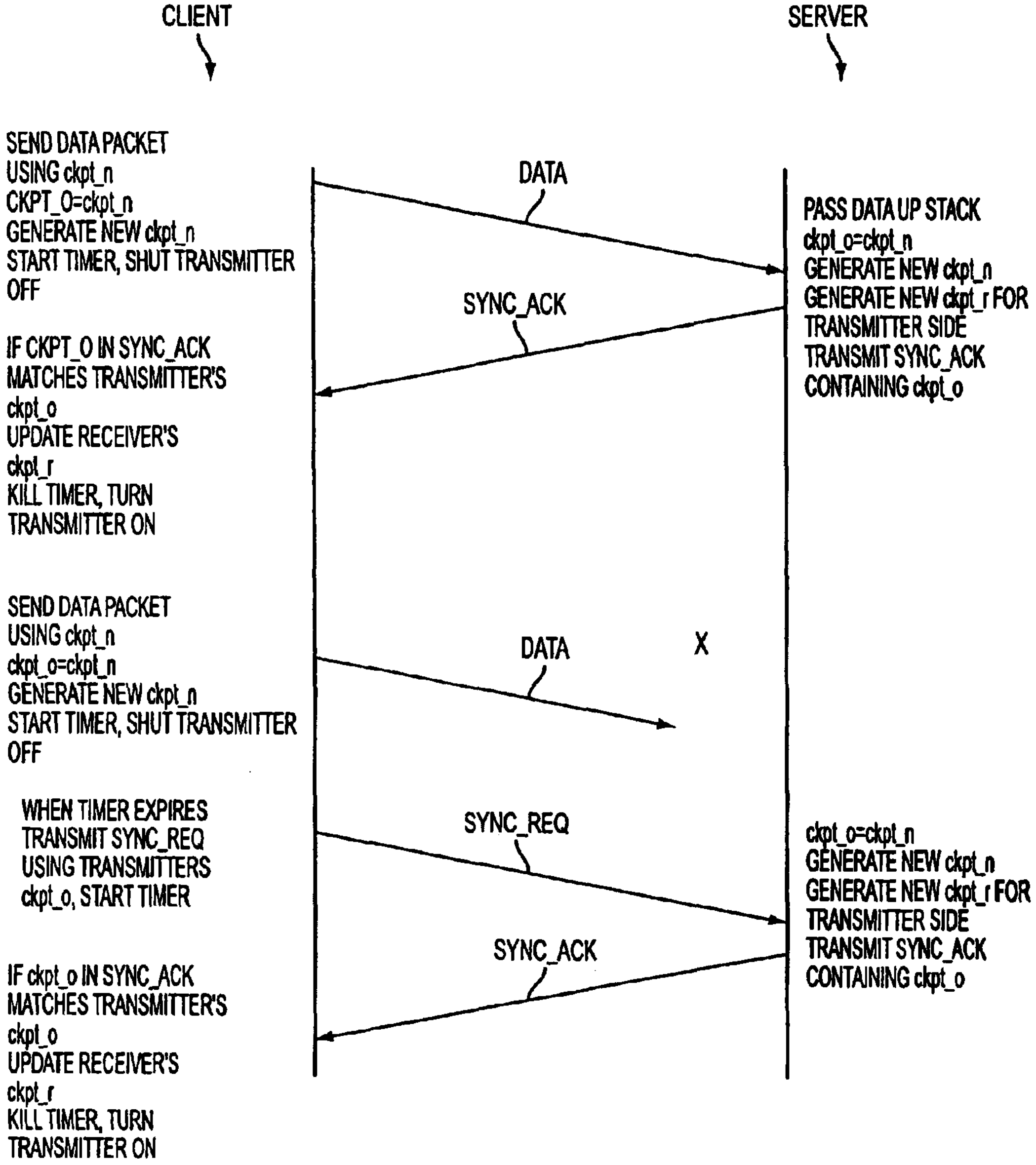

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER
OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR
TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
ckpt_o
UPDATE RECEIVER'S
ckpt_r
KILL TIMER, TURN
TRANSMITTER ON
SEND DATA PACKET
USING ckpt_n
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER
OFF
DATA
X
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS
ckpt_o, START TIMER
SYNC_REQ
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR
TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING ckpt_o
SYNC_ACK
IF ckpt_o IN SYNC_ACK
MATCHES TRANSMITTER'S
ckpt_o
UPDATE RECEIVER'S
ckpt_r
KILL TIMER, TURN
TRANSMITTER ON

FIG. 32

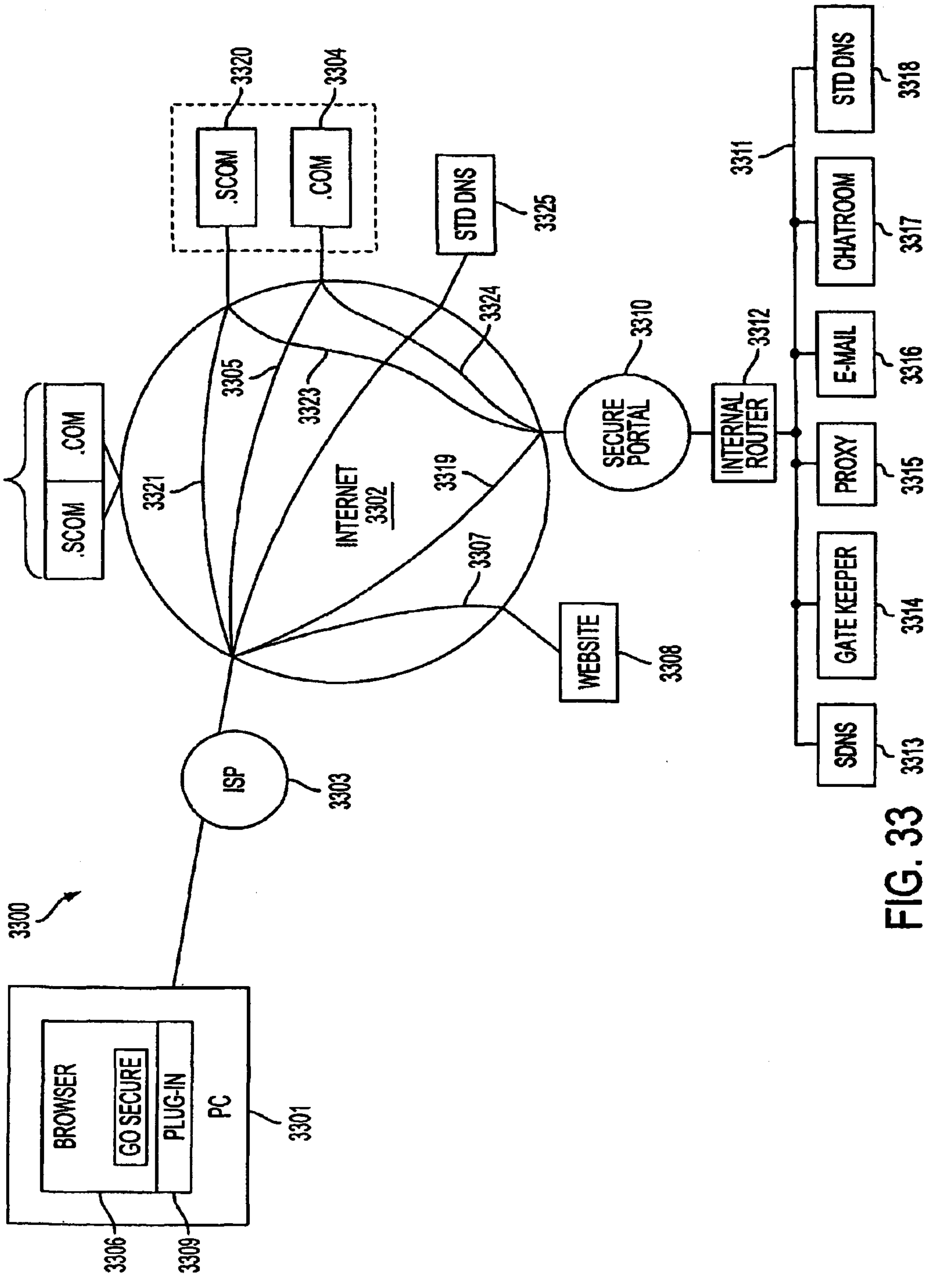

3300
BROWSER
GO SECURE
PLUG-IN
PC
3301
3306
3309
ISP
3303
INTERNET
3302
3321
3305
3323
3319
3307
3324
3322
.SCOM
.COM
3320
3304
.SCOM
.COM
STD DNS
3325
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
SDNS
3313
GATE KEEPER
3314
PROXY
3315
E-MAIL
3316
CHATROOM
3317
STD DNS
3318

FIG. 33

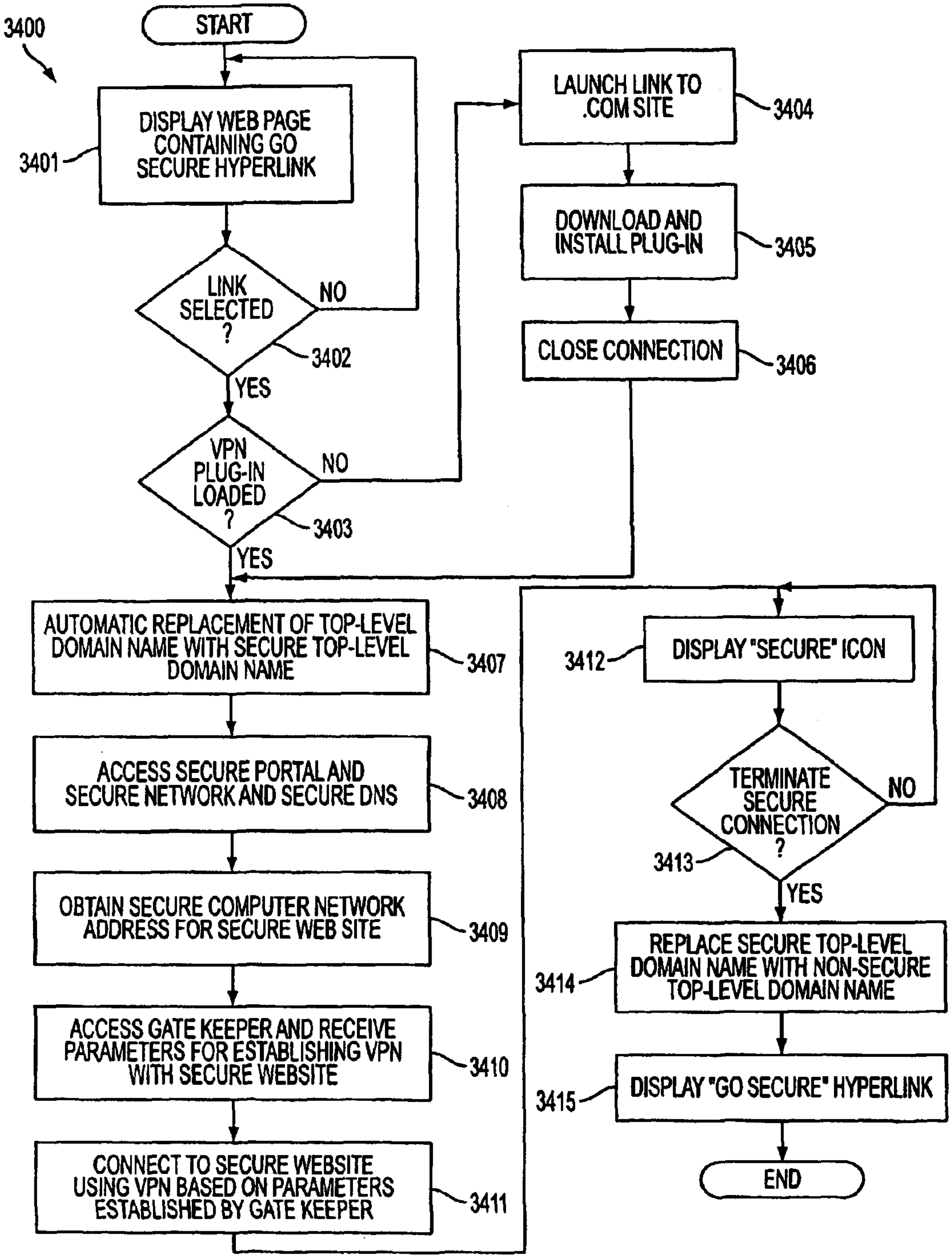

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED ?
NO
3402
YES
VPN PLUG-IN LOADED ?
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE PORTAL AND SECURE NETWORK AND SECURE DNS
3408
OBTAIN SECURE COMPUTER NETWORK ADDRESS FOR SECURE WEB SITE
3409
ACCESS GATE KEEPER AND RECEIVE PARAMETERS FOR ESTABLISHING VPN WITH SECURE WEBSITE
3410
CONNECT TO SECURE WEBSITE USING VPN BASED ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION ?
NO
3413
YES
REPLACE SECURE TOP-LEVEL DOMAIN NAME WITH NON-SECURE TOP-LEVEL DOMAIN NAME
3414
3415
DISPLAY "GO SECURE" HYPERLINK
END

FIG. 34

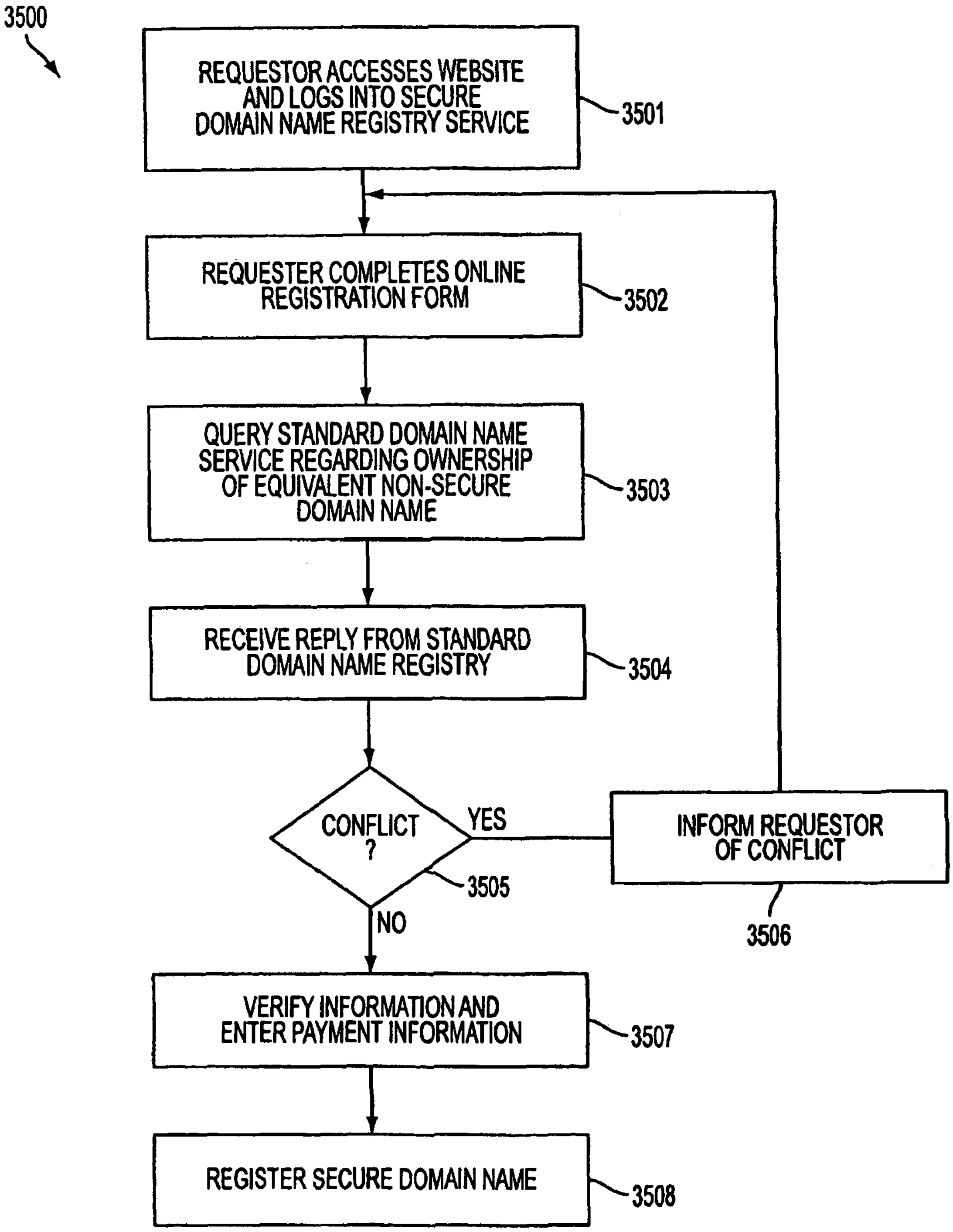

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
YES
3505
NO
INFORM REQUESTOR OF CONFLICT
3506
VERIFY INFORMATION AND ENTER PAYMENT INFORMATION
3507
REGISTER SECURE DOMAIN NAME
3508

FIG. 35

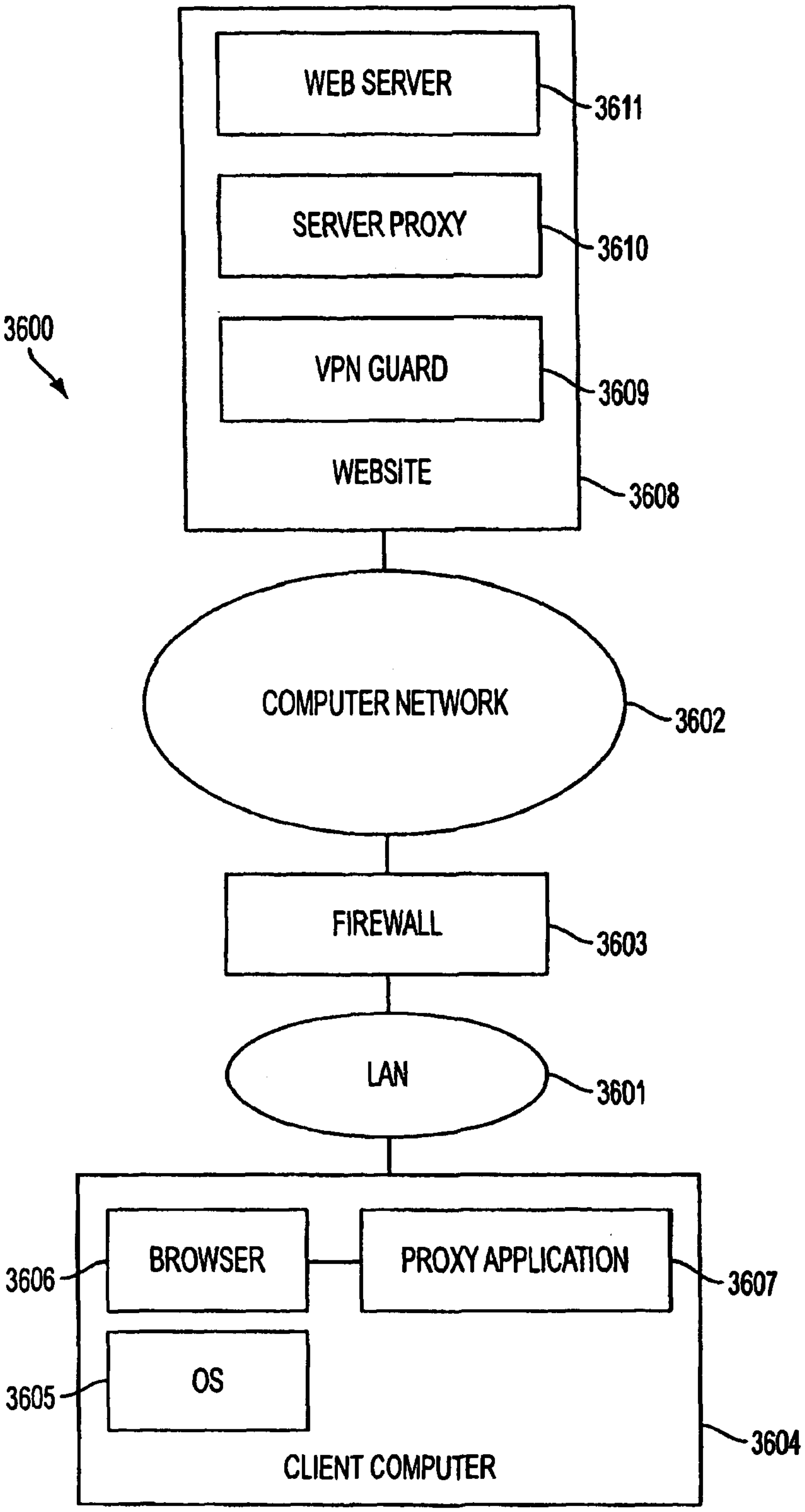

WEB SERVER
3611
SERVER PROXY
3610
3600
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
3606
BROWSER
PROXY APPLICATION
3607
3605
OS
3604
CLIENT COMPUTER

FIG. 36

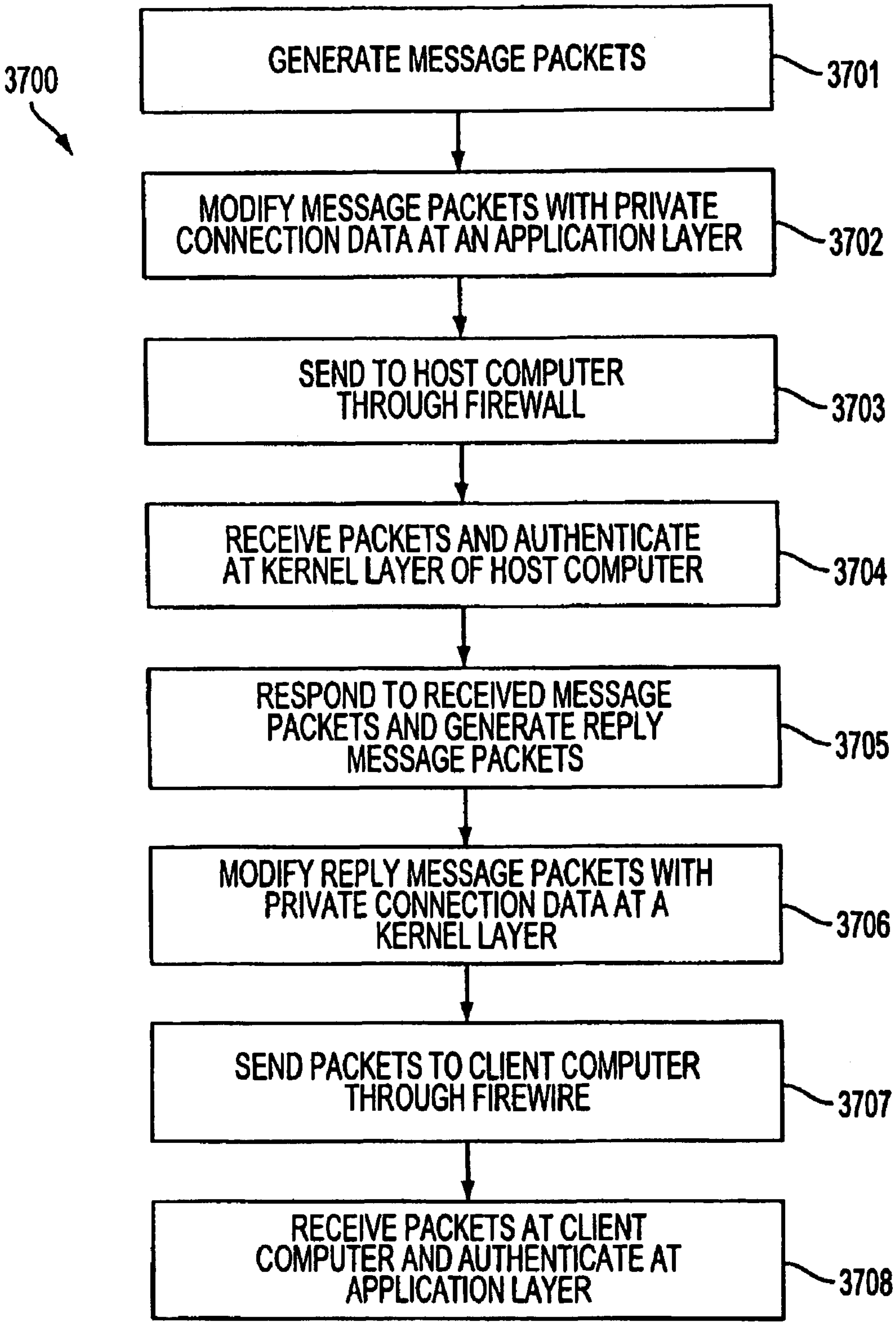

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS
3705
MODIFY REPLY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT A KERNEL LAYER
3706
SEND PACKETS TO CLIENT COMPUTER THROUGH FIREWIRE
3707
RECEIVE PACKETS AT CLIENT COMPUTER AND AUTHENTICATE AT APPLICATION LAYER
3708

FIG. 37

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from and is a divisional patent application of U.S. application Ser. No. 09/558,209, filed Apr. 26, 2000 and now abandoned, which is in turn a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/504,783, filed on Feb. 15, 2000 and now U.S. Pat. No. 6,502,135, issued Dec. 31, 2002, which in turn claims priority from and is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999, now U.S. Pat. No. 7,010,604, issued Mar. 7, 2006. The subject matter of U.S. application Ser. No. 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application No. 60/106,261 (filed Oct. 30, 1998) and Ser. No. 60/137,704 (filed Jun. 7, 1999). The present application is also related to U.S. application Ser. No. 09/558,210, filed Apr. 26, 2000 and now abandoned, which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. **1**. Two terminals, an originating terminal **100** and a destination terminal **110** are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal **100** may transmit secret information to terminal **110** over the Internet **107**. Also, it may be desired to prevent an eavesdropper from discovering that terminal **100** is in communication with terminal **110**. For example, if terminal **100** is a user and terminal **110** hosts a web site, terminal **100**'s user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

Data security is usually tackled using some form of data encryption. An encryption key **48** is known at both the originating and terminating terminals **100** and **110**. The keys may be private and public at the originating and destination terminals **100** and **110**, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet **140** undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called agile routing. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

The IP address of a TARP router can be changed, a feature called IP agility. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IP_T are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security. Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities

The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer.

According to another aspect of the invention, a command is entered to define a setup parameter associated with the secure communication link mode of communication. Consequently, the secure communication mode is automatically established when a communication link is established over the computer network.

The present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network. A non-standard top-level domain name is then sent over the virtual private network communication to a predetermined computer network address, such as a computer network address for a secure domain name service (SDNS).

The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

The present invention provides a way to encapsulate existing application network traffic at the application layer of a client computer so that the client application can securely communicate with a server protected by an agile network protocol. The advantages of the present invention are provided by a method for communicating using a private communication link between a client computer and a server computer over a computer network, such as the Internet. According to the invention, an information packet is sent from the client computer to the server computer over the computer network. The information packet contains data that is inserted into the payload portion of the packet at the application layer of the client computer and is used for forming a virtual private connection between the client computer and the server computer. The modified information packet can be sent through a firewall before being sent over the computer network to the server computer and by working on top of existing protocols (i.e., UDP, ICMP and TCP), the present invention more easily penetrates the firewall. The information packet is received at a kernel layer of an operating system on the server side. It is then determined at the kernel layer of the operating system on the host computer whether the information packet contains the data that is used for forming the virtual private connection. The server side replies by sending an information packet to the client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet.

Alternative, both information packets could be a TCP/IP protocol information packet, or an ICMP protocol information packet.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an illustration of secure communications over the Internet according to a prior art embodiment.

FIG. **2** is an illustration of secure communications over the Internet according to a an embodiment of the invention.

FIG. *3a* is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

FIG. *3b* is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

FIG. **4** is an illustration of an OSI layer location of processes that may be used to implement the invention.

FIG. **5** is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

FIG. **6** is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

FIG. **7** is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

FIG. **8** shows how a secure session is established and synchronized between a client and a TARP router.

FIG. **9** shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

FIG. **10** shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

FIG. **11** shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

FIG. **12**A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

FIG. **12**B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

FIG. **13** shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

FIG. **14** shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

FIG. **15** shows further details of the checkpoint scheme of FIG. **14**.

FIG. **16** shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

FIG. **17** shows a storage array for a receiver's active addresses.

FIG. **18** shows the receiver's storage array after receiving a sync request.

FIG. **19** shows the receiver's storage array after new addresses have been generated.

FIG. **20** shows a system employing distributed transmission paths.

FIG. **21** shows a plurality of link transmission tables that can be used to route packets in the system of FIG. **20**.

FIG. **22**A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

FIG. **22**B shows a flowchart for setting a weight value to zero if a transmitter turns off.

FIG. **23** shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

FIG. **24** shows an example using the system of FIG. **23**.

FIG. **25** shows a conventional domain-name look-up service.

FIG. **26** shows a system employing a DNS proxy server with transparent VPN creation.

FIG. **27** shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

FIG. **28** shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

FIG. **29** shows one embodiment of a system employing the principles of FIG. **28**.

FIG. **30** shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

FIG. **31** shows a signaling server **3101** and a transport server **3102** used to establish a VPN with a client computer.

FIG. **32** shows message flows relating to synchronization protocols of FIG. **31**.

FIG. **33** shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use.

FIG. **34** shows a flow diagram for installing and establishing a "one-click" secure communication link over a computer network according to the present invention.

FIG. **35** shows a flow diagram for registering a secure domain name according to the present invention.

FIG. **36** shows a system block diagram of a computer network in which a private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks.

FIG. **37** shows a flow diagram for establishing a virtual private connection that is encapsulated using an existing network protocol.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. **2**, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers **122-127** that are similar to regular IP routers **128-132** in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets **140**. TARP packets **140** are identical to normal IP packet messages that are routed by regular IP routers **128-132** because each TARP packet **140** contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's **140** IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal **110**. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet **140** since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal **110**.

Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key **146**. The link key **146** is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal **100** and the destination TARP terminal **110**. Each TARP router **122-127**, using the link key **146** it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key **146** and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

Once the outer layer of decryption is completed by a TARP router **122-127**, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet **140** to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet **140** to another TARP router **122-127** or to the destination TARP terminal **110**. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet **140** may forward the TARP packet **140** to the destination TARP terminal **110**. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet **140** may forward the TARP packet **140** to a TARP router **122-127** that the current TARP terminal chooses at random. As a result, each TARP packet **140** is routed through some minimum number of hops of TARP routers **122-127** which are chosen at random.

Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called agile routing. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IP_C. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers **122-127** intervening between the originating **100** and destination **110** TARP terminals. The session key is used to decrypt the payloads of the TARP packets **140** permitting an entire message to be reconstructed.

In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets **140** may be used as desired.

Referring to FIG. **3***a*, to construct a series of TARP packets, a data stream **300** of IP packets **207***a*, **207***b*, **207***c*, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments **1-9** are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets **207a-207c** used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the interleave window.

To create a packet, the transmitting software interleaves the normal IP packets **207***a* et. seq. to form a new set of interleaved payload data **320**. This payload data **320** is then encrypted using a session key to form a set of session-key-encrypted payload data **330**, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets **207***a*-**207***c*, new TARP headers IP_T are formed. The TARP headers IP_T can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.
2. An interleave sequence number—an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.
3. A time-to-live (TTL) datum—indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.
4. Data type identifier—indicates whether the payload contains, for example, TCP or UDP data.
5. Sender's address—indicates the sender's address in the TARP network.
6. Destination address—indicates the destination terminal's address in the TARP network.
7. Decoy/Real—an indicator of whether the packet contains real message data or dummy decoy data or a combination.

Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets **207***a*-**207***c* all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

Referring to FIG. **3***b*, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block **520** for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. **3***b*. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of FIG. **3***a*. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. **3***a*. The remaining process is as shown in, and discussed with reference to, FIG. **3***a*.

Once the TARP packets **340** are formed, each entire TARP packet **340**, including the TARP header IP_T, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IP_C is added to each encrypted TARP packet **340** to form a normal IP packet **360** that can be transmitted to a TARP router. Note that the process of constructing the TARP packet **360** does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. **4**, a TARP transceiver **405** can be an originating terminal **100**, a destination terminal **110**, or a TARP router **122-127**. In each TARP Transceiver **405**, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver **405** is a router, the received TARP packets **140** are not processed into a stream of IP packets **415** because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal **110**. The intervening process, a "TARP Layer" **420**, could be combined with either the data link layer **430** or the Network layer **410**. In either case, it would intervene between the data link layer **430** so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer **410**. As an example of combining the TARP layer **420** with the data link layer **430**, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

Decoy packets may be generated by each TARP terminal **100**, **110** or each router **122-127** on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal **110** may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

Referring to FIG. **5**, the following particular steps may be employed in the above-described method for routing TARP packets.

S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.

S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S4. If the packet is a decoy packet, the perishable decoy counter is incremented.

S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.

S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.

S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.

S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.

S10. The TARP packet is encrypted using the memorized link key.

S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

Referring to FIG. 6, the following particular steps may be employed in the above-described method for generating TARP packets.

S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.

S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.

S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.

S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.

S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.

S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

Referring to FIG. 7, the following particular steps may be employed in the above-described method for receiving TARP packets.

S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.

S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S44. If the packet is a decoy packet, the perishable decoy counter is incremented.

S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.

S46. The TARP packets are cached until all packets forming an interleave window are received.

S47. Once all packets of an interleave window are received, the packets are deinterleaved.

S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.

S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.

S50. The packets are then handed up to the IP layer processes.

1. Scalability Enhancements

The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

FIG. **8** shows how a client computer **801** and a TARP router **811** can establish a secure session. When client **801** seeks to establish an IHOP session with TARP router **811**, the client **801** sends "secure synchronization" request ("SSYN") packet **821** to the TARP router **811**. This SYN packet **821** contains the client's **801** authentication token, and may be sent to the router **811** in an encrypted format. The source and destination IP numbers on the packet **821** are the client's **801** current fixed IP address, and a "known" fixed IP address for the router **811**. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's **801** SSYN packet **821**, the router **811** responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") **822** to the client **801**. This SSYN ACK **822** will contain the transmit and receive hopblocks that the client **801** will use when communicating with the TARP router **811**. The client **801** will acknowledge the TARP router's **811** response packet **822** by generating an encrypted SSYN ACK ACK packet **823** which will be sent from the client's **801** fixed IP address and to the TARP router's **811** known fixed IP address. The client **801** will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet **824**, will be sent with the first {sender, receiver} IP pair in the client's transmit table **921** (FIG. **9**), as specified in the transmit hopblock provided by the TARP router **811** in the SSYN ACK packet **822**. The TARP router **811** will respond to the SSI packet **824** with an SSI ACK packet **825**, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table **923**. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client **801** and the TARP router **811** will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client **801** and TARP router **802** may re-establish the secure session by the procedure outlined in FIG. **8** and described above.

While the secure session is active, both the client **901** and TARP router **911** (FIG. **9**) will maintain their respective transmit tables **921**, **923** and receive tables **922**, **924**, as provided by the TARP router during session synchronization **822**. It is important that the sequence of IP pairs in the client's transmit table **921** be identical to those in the TARP router's receive table **924**; similarly, the sequence of IP pairs in the client's receive table **922** must be identical to those in the router's transmit table **923**. This is required for the session synchronization to be maintained. The client **901** need maintain only one transmit table **921** and one receive table **922** during the course of the secure session. Each sequential packet sent by the client **901** will employ the next { send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router **911** will expect each packet arriving from the client **901** to bear the next IP address pair shown in its receive table.

Since packets can arrive out of order, however, the router **911** can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router **911** to the client **901** are maintained in an identical manner; in particular, the router **911** will select the next IP address pair from its transmit table **923** when constructing a packet to send to the client **901**, and the client **901** will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link-based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of FIG. **9**; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in FIG. **10**, for example, client **1001** can establish three simultaneous sessions with each of three TARP routers provided by different ISPs **1011**, **1012**, **1013**. As an example, the client **1001** can use three different telephone lines **1021**, **1022**, **1023** to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of-service attacks and traffic monitoring.

2. Further Extensions

The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. **11**, for example, a first Ethernet frame **1150** comprises a frame header **1101** and two embedded IP packets IPI and IP**2**, while a second Ethernet frame **1160** comprises a different frame header **1104** and a single IP packet IP**3**. Each frame header generally includes a source hardware address **1101**A and a destination hardware address **1101**B; other well-known fields in frame headers are omitted from FIG. **11** for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

FIG. 12A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

As shown in FIG. 12A, two computer nodes **1201** and **1202** communicate over a communication channel such as an Ethernet. Each node executes one or more application programs **1203** and **1218** that communicate by transmitting packets through communication software **1204** and **1217**, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software **1204** and **1217** can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

The lowest levels of communication software **1204** and **1217** communicate with hardware components **1206** and **1214** respectively, each of which can include one or more registers **1207** and **1215** that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if all of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

Reference will now be made to FIGS. **12A** and **12B** in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes **1201** and **1202** are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (**1204** and **1217**, respectively) contains a modified element **1205** and **1216** that performs certain functions that deviate from the standard communication protocols. In particular, computer node **1201** implements a first "hop" algorithm **1208X** that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node **1201** maintains a transmit table **1208** containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node **1202**. As each new IP packet is formed, the next sequential entry out of the sender's transmit table **1208** is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

At the receiving node **1202**, the same IP hop algorithm **1222X** is maintained and used to generate a receive table **1222** that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table **1208** matching the second five entries of receive table **1222**. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node **1202** maintains a receive window **W3** that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window **W3** slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window **W3** will be accepted; those falling outside of window **W3** will be rejected as invalid. The length of window **W3** can be adjusted as necessary to reflect network delays or other factors.

Node **1202** maintains a similar transmit table **1221** for creating IP packets and frames destined for node **1201** using a potentially different hopping algorithm **1221X**, and node **1201** maintains a matching receive table **1209** using the same algorithm **1209X**. As node **1202** transmits packets to node **1201** using seemingly random IP source, IP destination, and/or discriminator fields, node **1201** matches the incoming packet values to those falling within window WI maintained in its receive table. In effect, transmit table **1208** of node **1201** is synchronized (i.e., entries are selected in the same order) to receive table **1222** of receiving node **1202**. Similarly, transmit table **1221** of node **1202** is synchronized to receive table **1209** of node **1201**. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. **12A** (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node **1201** further maintains a transmit table **1210** using a transmit algorithm **1210X** to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields **1101A** and **1101B** in FIG. **11**) that are synchronized to a corresponding receive table **1224** at node **1202**. Similarly, node **1202** maintains a different transmit table **1223** containing source and destination hardware addresses that is synchronized with a corresponding receive table **1211** at node **1201**. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

FIG. **12B** shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. 12A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "deadman" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair—and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

The aforementioned scheme may have some inherent security issues associated with it—namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair;

this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. **13**, where (for example) a first ISP **1302** is the sender and a second ISP **1303** is the receiver. (Other alternatives are possible from FIG. **13**.) A transmitted packet comprises a public or "outer" header **1305** that is not encrypted, and a private or "inner" header **1306** that is encrypted using for example a link key. Outer header **1305** includes a public sync portion while inner header **1306** contains the private sync portion. A receiving node decrypts the inner header using a decryption function **1307** in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step **1308**.) The public and decrypted private sync portions are combined in function **1308** in order to generate the combined sync **1309**. The combined sync (**1309**) is then fed into the RNG (**1310**) and compared to the IP address pair (**1311**) to validate or reject the packet.

An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent—even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. **14**):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.
3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. **14**).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. **15**. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack , at which point transmission is reestablished.

From the receiver's perspective, the scheme operates as follows: (1) when it receives a sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it will actually help to re-establish synchronization.

A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead Capability

An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead n steps efficiently. An LCR generates random numbers X_1, X_2, X_3 . . . X_k starting with seed X_0 using a recurrence

$$X_1=(a\,X_{i-1}+b) \bmod c, \tag{1}$$

where a, b and c define a particular LCR. Another expression for X_i,

$$X_i=((a^i(X_0+b)-b)/(a-1)) \bmod c \tag{2}$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c. \tag{3}$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c=((a^i \bmod((a-1)c)(X_0(a-1)+b)-b)/(a-1)) \bmod c \tag{4}.$$

$(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute $a^i \bmod((a-1)c)$ (this requires O(log(i)) steps).

A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every n packets. The window would commence n IP pairs from the start of the previous window. Using X_j^w, the random number at the j^{th} checkpoint, as X_0 and n as i, a node can store $a^n \bmod((a-1)c)$ once per LCR and set

$$X_{j+1}^w=X_{n(j+1)}=((a^n \bmod((a-1)c)(X_j^w(a-1)+b)-b)/(a-1))\bmod c, \tag{5}$$

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n). Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack-against the encryptor.

F. Random Number Generator Example

Consider a RNG where a=31, b=4 and c=15. For this case equation (1) becomes:

$$X_i=(31\,X_{i-1}+4) \bmod 15. \tag{6}$$

If one sets X_0=1, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence a^n=313=29791, c*(a−1)=15*30=450 and a^n mod ((a−1)c)=31^3mod(15*30)=29791 mod(450)=91. Equation (5) becomes:

$$((91(X_i30+4)-4)/30)\bmod 15 \tag{7}.$$

Table 1 shows the jump ahead calculations from (7). The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	$(X_i30 + 4)$	$91\ (X_i30 + 4) - 4$	$((91\ (X_i30 + 4) - 4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).
3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B-trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n-1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the x^{th} bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

For example, suppose one wanted to represent the number 135 using a presence vector. The 135^{th} bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135^{th} bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. **16**). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

A presence vector will have a 1 in the y^{th} bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

I. Further Synchronization Enhancements

A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2×WINDOW_SIZE+OoO active addresses (1≦OoO≦WINDOW_SIZE and WINDOW_SIZE≧1). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. **17** depicts a storage array for a receiver's active addresses.

The receiver starts with the first 2×WINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as "used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last initial transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. **18** when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

FIG. **19** shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2×WINDOW_SIZE−OoO then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

1. There is no need for an efficient jump ahead in the random number generator,
2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

Another embodiment incorporating various inventive principles is shown in FIG. **20**. In this embodiment, a message transmission system includes a first computer **2001** in communication with a second computer **2002** through a network **2011** of intermediary computers. In one variant of this embodiment, the network includes two edge routers **2003** and **2004** each of which is linked to a plurality of Internet Service Providers (ISPs) **2005** through **2010**. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. **20**, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. **20** to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element **2005**) to ISP D (element **2008**)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

As shown in FIG. **21**, computer **2001** or edge router **2003** incorporates a plurality of link transmission tables **2100** that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table **2101** contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer **2001** to second computer **2002**, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element **2005**) and ISP B (element **2008**)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link table can be set to a "down" condition as shown in table **2105**, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. Continuation-in-Part Improvements

The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities. Each is discussed separately below.

A. Load Balancer

Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. **20** and **21** and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

FIG. **22**A shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. **22**A. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

Beginning in step **2201**, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

In step **2202**, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step **2201**.

In step **2203**, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step **2207** a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step **2209** the weight is set to the minimum level and processing resumes at step **2201**. If the weight is above the minimum level, then in step **2208** the weight is gradually decreased for the path, then in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

If in step **2203** the quality of the path was greater than or equal to the threshold, then in step **2204** a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step **2205** the weight is increased toward the steady-state value, and in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step **2204** the weight is not less than the steady-state value, then processing resumes at step **2201** without adjusting the weights.

The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

Although not explicitly shown in FIG. **22**A the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

FIG. **22**B shows steps that can be executed to shut down transmission links where a transmitter turns off. In step **2210**, a transmitter shut-down event occurs. In step **2211**, a test is made to determine whether at least one transmitter is still turned on. If not, then in step **2215** all packets are dropped until a transmitter turns on. If in step **2211** at least one transmitter is turned on, then in step **2212** the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

FIG. **23** shows a computer node **2301** employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. **23** communicate over a plurality of separate physical transmission paths. As shown in FIG. **23**, four transmission paths X1 through X4 are defined for communicating between the two nodes. Each node includes a packet transmitter **2302** that operates in accordance with a transmit table **2308** as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver **2303** that operates in accordance with a receive table **2309**, including a moving window W that moves as valid packets are received. Invalid packets having source and destination addresses that do not fall within window W are rejected.

As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table **2308** according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch **2307**. Switch **2307**, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table **2306**. For example, if the weight for path X1 is 0.2, then every fifth packet will be transmitted on path X1. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

Packet receiver **2303** generates an output to a link quality measurement function **2304** that operates as described above to determine the quality of each transmission path. (The input to packet receiver **2303** for receiving incoming packets is omitted for clarity). Link quality measurement function **2304** compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function **2305**. If a weight adjustment is required, then the weights in table **2306** are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

Link quality measurement function **2304** can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function **2304**. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This allows the transmitter to compare messages sent to messages received in order to assess the health of the link.

If synchronization is completely lost, weight adjustment function **2305** decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to:

$$P'=\alpha\times\text{MIN}+(1-\alpha)\times P \qquad (1)$$

Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to:

$$P'=\beta\times S+(1-\beta)\times P \qquad (2)$$

where β is a parameter such that 0<=β<=1 that determines the damping rate of P.

Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

A detailed example will now be provided with reference to FIG. **24**. As shown in FIG. **24**, a first computer **2401** communicates with a second computer **2402** through two routers **2403** and **2404**. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

Suppose that a first link L**1** can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L**2** can sustain 75 Mb/s and has a window size of 24; and link L**3** can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200 Mb/s. The steady state traffic weights are 0.5 for link L**1**; 0.375 for link L**2**, and 0.125 for link L**3**. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, α=0.75 and β=0.5. These traffic weights will remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L**1** receives a SYNC_ACK containing a MESS_R of **24**, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link **1** would be below THRESH (0.8). Consequently, link L**1**'s traffic weight value would be reduced to 0.12825, while link L**2**'s traffic weight value would be increased to 0.65812 and link L**3**'s traffic weight value would be increased to 0.217938.

2. Link L**2** and L**3** remained healthy and link L**1** stopped to synchronize. Then link L**1**'s traffic weight value would be set to 0, link L**2**'s traffic weight value would be set to 0.75, and link L**33**'s traffic weight value would be set to 0.25.

3. Link L**1** finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L**1** would be below THRESH. Link L**1**'s traffic weight value would be increased to 0.005, link L**2**'s traffic weight value would be decreased to 0.74625, and link L**3**'s traffic weight value would be decreased to 0.24875.

4. Link L**1** received a SYNC_ACK containing a MESS_R of **32** indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L**1** would be above THRESH. Link L**1**'s traffic weight value would be increased to 0.2525, while link L**2**'s traffic weight value would be decreased to 0.560625 and link L**3**'s traffic weight value would be decreased to 0.186875.

5. Link L**1** received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L**1** would be above THRESH. Link L**1**'s traffic weight value would be increased to 0.37625; link L**2**'s traffic weight value would be decreased to 0.4678125, and link L**3**'s traffic weight value would be decreased to 0.1559375.

6. Link L**1** remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

This conventional scheme is shown in FIG. **25**. A user's computer **2501** includes a client application **2504** (for example, a web browser) and an IP protocol stack **2505**. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack **2505**) to a DNS **2502** to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application

2504, which is then able to use the IP address to communicate with the host **2503** through separate transactions such as PAGE REQ and PAGE RESP.

In the conventional architecture shown in FIG. **25**, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

FIG. **26** shows a system employing various principles summarized above. A user's computer **2601** includes a conventional client (e.g., a web browser) **2605** and an IP protocol stack **2606** that preferably operates in accordance with an IP hopping function **2607** as outlined above. A modified DNS server **2602** includes a conventional DNS server function **2609** and a DNS proxy **2610**. A gatekeeper server **2603** is interposed between the modified DNS server and a secure target site **2704**. An "unsecure" target site **2611** is also accessible via conventional IP protocols.

According to one embodiment, DNS proxy **2610** intercepts all DNS lookup functions from client **2605** and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy **2610** determines whether the user has sufficient security privileges to access the site. If so, DNS proxy **2610** transmits a message to gatekeeper **2603** requesting that a virtual private network be created between user computer **2601** and secure target site **2604**. In one embodiment, gatekeeper **2603** creates "hopblocks" to be used by computer **2601** and secure target site **2604** for secure communication. Then, gatekeeper **2603** communicates these to user computer **2601**. Thereafter, DNS proxy **2610** returns to user computer **2601** the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) **2604**, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site **2611**, DNS proxy would merely pass through to conventional DNS server **2609** the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site **2611**. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy **2610** would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

Gatekeeper **2603** can be implemented on a separate computer (as shown in FIG. **26**) or as a function within modified DNS server **2602**. In general, it is anticipated that gatekeeper **2703** facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site **2604** are assumed to be equipped with a secure communication function such as an IP hopping function **2608**.

It will be appreciated that the functions of DNS proxy **2610** and DNS server **2609** can be combined into a single server for convenience. Moreover, although element **2602** is shown as combining the functions of two servers, the two servers can be made to operate independently.

FIG. **27** shows steps that can be executed by DNS proxy server **2610** to handle requests for DNS look-up for secure hosts. In step **2701**, a DNS look-up request is received for a target host. In step **2702**, a check is made to determine whether access to a secure host was requested. If not, then in step **2703** the DNS request is passed to conventional DNS server **2609**, which looks up the IP address of the target site and returns it to the user's application for further processing.

In step **2702**, if access to a secure host was requested, then in step **2704** a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper **2603** (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

If the user is not authorized to access the secure site, then a "host unknown" message is returned (step **2705**). If the user has sufficient security privileges, then in step **2706** a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

Some or all of the security functions can be embedded in gatekeeper **2603**, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy **2610** communicates with gatekeeper **2603** to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:

Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would reject the request, informing DNS proxy server **2610** that it was unable to find the target computer. The DNS proxy **2610** would then return a "host unknown" error message to the client.

Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server **2610**, which would check its rules and determine that no VPN is needed. Gatekeeper **2603** would then inform the DNS proxy server to forward the request to conventional DNS server **2609**, which would resolve the request and return the result to the DNS proxy server and then back to the client.

Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper **2603**. Gatekeeper **2603** would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server **2610** to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. **28**, suppose that a first host computer **2801** is communicating with a second host computer **2804** using the IP address hopping principles described above. The first host computer is coupled through an edge router **2802** to an Internet Service Provider (ISP) **2803** through a low bandwidth link (LOW BW), and is in turn coupled to second host computer **2804** through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router **2802**.

Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer **2801** across high bandwidth link HIGH BW. Normally, host computer **2801** would be able to quickly reject the packets since they would not fall within the acceptance window permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer **2801**. Consequently, the link to host computer **2801** is effectively flooded before the packets can be discarded.

According to one inventive improvement, a "link guard" function **2805** is inserted into the high-bandwidth node (e.g., ISP **2803**) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc **2401**], the packets have IP protocols **420** and **421**. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, **2805**, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid. According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP **2903** maintains a copy **2910** of the receive table used by host computer **2901**. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard **2805** validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc **2104**].

According to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

As shown in FIG. **29**, for example, suppose that a first host computer **2900** is communicating with a second host computer **2902** over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP **2901** and a low bandwidth link LOW BW through an edge router **2904**. In accordance with the basic architecture described above, first host computer **2900** and second host computer **2902** would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables **2905**, **2906**, **2912** and **2913**. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

Suppose that a nefarious computer hacker **2903** was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP **2901**, and that these packets are being forwarded over a low-bandwidth link. Hacker computer **2903** could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer **3000** would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard **2911** would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

According to one embodiment of the improvement, ISP **2901** maintains a separate VPN with first host computer **2900**, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer **2900**. The cryptographic keys used to authenticate VPN packets at the link guard **2911** and the cryptographic keys used to encrypt and decrypt the VPN packets at host **2902** and host **2901** can be different, so that link guard **2911** does not have access to the private host data; it only has the capability to authenticate those packets.

According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard **2911** can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively control the rate at which its hopping window moves by delaying "SYNC ACK" responses to "SYNC_REQ" messages.

A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT_N. It is a simple matter of deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate, each receiver could defer issuing a new CKPT_N until M×N×W/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will reissue the SYNC_REQ every T1 seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

Two practical issues should be considered when implementing the above scheme:

1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing for a period (e.g. the network dropping a SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of M×N×W/R seconds after the last SYNC_REQ has been received and accepted, 2×M×N×W/R seconds after next to the last SYNC_REQ has been received and accepted, C×M×N×W/R seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

FIG. **30** shows a system employing the above-described principles. In FIG. **30**, two computers **3000** and **3001** are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer **3000** will be referred to as the receiving computer and computer **3001** will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver **3000**.

As described above, receiving computer **3000** maintains a receive table **3002** including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer **3001** maintains a transmit table **3003** from which the next IP address pairs will be selected when transmitting a packet to receiving computer **3000**. (For the sake of illustration, window W is also illustrated with reference to transmit table **3003**). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function **3010**. This is a request to receiver **3000** to synchronize the receive table **3002**, from which transmitter **3001** expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer **3001** transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver **3000** will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter **3001** will be discarded).

In accordance with the improvements described above, receiving computer **3000** performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. **30**. In step **3004**, receiving computer **3000** receives the SYNC_REQ message. In step **3005**, a check is made to determine whether the request is a duplicate. If so, it is discarded in step **3006**. In step **3007**, a check is made to determine whether the SYNC_REQ received from transmitter **3001** was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step **3008** the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

Otherwise, if the rate has not been exceeded, then in step **3109** the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from the transmitter **3101**. Transmitter **3101** then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

FIG. **31** shows a system employing certain of the above-described principles. In FIG. **31**, a signaling server **3101** and a transport server **3102** communicate over a link. Signaling server **3101** contains a large number of small tables **3106** and **3107** that contain enough information to authenticate a communication request with one or more clients **3103** and **3104**. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server **3102**, which is preferably a separate computer in communication with signaling server **3101**, contains a smaller number of larger hopping tables **3108**, **3109**, and **3110** that can be allocated to create a VPN with one of the client computers.

According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server **3101** will quickly reject invalid packets from unauthorized computers such as hacker computer **3105**. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server **3101** with bogus packets. Details of this scheme are provided below.

Signaling server **3101** receives the request **3111** and uses it to determine that client **3103** is a validly registered user. Next, signaling server **3101** issues a request to transport server **3102** to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client **3103**. The allocated hopping parameters are returned to signaling server **3101** (path **3113**), which then supplies the hopping parameters to client **3103** via path **3114**, preferably in encrypted form.

Thereafter, client **3103** communicates with transport server **3102** using the normal hopping techniques described above. It will be appreciated that although signaling server **3101** and transport server **3102** are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. **31** differently from as shown without departing from the inventive principles.

One advantage of the above-described architecture is that signaling server **3101** need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer **3105**. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server **3102**, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server **3102** or signaling server **3101**.

A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element **3106** in FIG. **31**.

The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer Ti noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.

2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and other information (i.e., user credentials) contained in the inner header It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.

4. T1 expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer Ti noting CKPT_O again, and a SYNC REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.

5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

FIG. **32** shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

The above-described procedures allow a client to be authenticated at signaling server **3201** while maintaining the ability of signaling server **3201** to quickly reject invalid packets, such as might be generated by hacker computer **3205**. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

F. One-Click Secure On-line Communications and Secure Domain Name Service

The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. **33** shows a system block diagram **3300** of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. **33**, a computer terminal or client computer **3301**, such as a personal computer (PC), is connected to a computer network **3302**, such as the Internet, through an ISP **3303**. Alternatively, computer **3301** can be connected to computer network **3302** through an edge router. Computer **3301** includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer **3301** can communicate conventionally with another computer **3304** connected to computer network **3302** over a communication link **3305** using a browser **3306** that is installed and operates on computer **3301** in a well-known manner.

Computer **3304** can be, for example, a server computer that is used for conducting e-commerce. In the situation when computer network **3302** is the Internet, computer **3304** typically will have a standard top-level domain name such as .com, .net, .org, .edu, .mil or .gov.

FIG. **34** shows a flow diagram **3400** for installing and establishing a "one-click" secure communication link over a computer network according to the present invention. At step **3401**, computer **3301** is connected to server computer **3304** over a non-VPN communication link **3305**. Web browser **3306** displays a web page associated with server **3304** in a well-known manner. According to one variation of the invention, the display of computer **3301** contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network **3302** between terminal **3301** and server **3304**. Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer **3304**, thereby indicating that the entity providing server **3304** also provides VPN capability.

By displaying the "go secure" hyperlink, a user at computer **3301** is informed that the current communication link between computer **3301** and server computer **3304** is a non-secure, non-VPN communication link. At step **3402**, it is determined whether a user of computer **3301** has selected the "go secure" hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step **3402**, it is determined that the user has selected the "go secure" hyperlink, flow continues to step **3403** where an object associated with the hyperlink determines whether a VPN communication software module has already been installed on computer **3301**. Alternatively, a user can enter a command into computer **3301** to "go secure."

If, at step **3403**, the object determines that the software module has been installed, flow continues to step **3407**. If, at step **3403**, the object determines that the software module has not been installed, flow continues to step **3404** where a non-VPN communication link **3307** is launched between computer **3301** and a website **3308** over computer network **3302** in a well-known manner. Website **3308** is accessible by all computer terminals connected to computer network **3302** through a non-VPN communication link. Once connected to website **3308**, a software module for establishing a secure communication link over computer network **3302** can be downloaded and installed. Flow continues to step **3405** where, after computer **3301** connects to website **3308**, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal **3301** as software module **3309**. At step **3405**, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network **3302**. At step **3406**, the -communication link between computer **3301** and website **3308** is then terminated in a well-known manner.

By clicking on the "go secure" hyperlink, a user at computer **3301** has enabled a secure communication mode of communication between computer **3301** and server computer **3304**. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer **3301** and server computer **3304** are performed transparently to a user at computer **3301**.

At step **3407**, a secure VPN communications mode of operation has been enabled and software module **3309** begins to establish a VPN communication link. In one embodiment, software module **3309** automatically replaces the top-level domain name for server **3304** within browser **3406** with a secure top-level domain name for server computer **3304**. For example, if the top-level domain name for server **3304** is .com, software module **3309** replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module **3409** can replace the top-level domain name of server **3304** with any other non-standard top-level domain name.

Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module **3409** contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module **3309** accesses a secure portal **3310** that interfaces a secure network **3311** to computer network **3302**. Secure network **3311** includes an internal router **3312**, a secure domain name service (SDNS) **3313**, a VPN gatekeeper **3314** and a secure proxy **3315**. The secure network can include other network services, such as e-mail **3316**, a plurality of chatrooms (of which only one chatroom **3317** is shown), and a standard domain name service (STD DNS) **3318**. Of course, secure network **3311** can include other resources and services that are not shown in FIG. **33**.

When software module **3309** replaces the standard top-level domain name for server **3304** with the secure top-level domain name, software module **3309** sends a query to SDNS **3313** at step **3408** through secure portal **3310** preferably using an administrative VPN communication link **3319**. In this configuration, secure portal **3310** can only be accessed using a VPN communication link. Preferably, such a VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence; an IP address hopping regime that pseudorandomly changes IP addresses in packets transmitted between a client computer and a secure target computer; periodically changing at least one field in a series of data packets according to a known sequence; an Internet Protocol (IP) address in a header of each data packet that is compared to a table of valid IP addresses maintained in a table in the second computer; and/or a comparison of the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window. Other types of VPNs can alternatively be used. Secure portal **3310** authenticates the query from software module **3309** based on the particular information hopping technique used for VPN communication link **3319**.

SDNS **3313** contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS **3313** stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS **3313** so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website.

Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure securities trading website. When a user queries SDNS **3313** for the secure computer network address for the securities trading website, SDNS **3313** determines the particular secure computer network address based on the user's identity and the user's subscription level.

At step **3409**, SDNS **3313** accesses VPN gatekeeper **3314** for establishing a VPN communication link between software module **3309** and secure server **3320**. Server **3320** can only be accessed through a VPN communication link. VPN gatekeeper **3314** provisions computer **3301** and secure web server computer **3320**, or a secure edge router for server computer **3320**, thereby creating the VPN. Secure server computer **3320** can be a separate server computer from server computer **3304**, or can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer **3322**. Returning to FIG. **34**, in step **3410**, SDNS **3313** returns a secure URL to software module **3309** for the scom server address for a secure server **3320** corresponding to server **3304**.

Alternatively, SDNS **3313** can be accessed through secure portal **3310** "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal **3310** preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS **3319**. Because the initial communication link in this situation is not a VPN communication link, the reply to the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS **3313** can be in the clear, and SDNS **3313** and gatekeeper **3314** can operate to establish a VPN communication link to the querying computer for sending the reply.

At step **3411**, software module **3309** accesses secure server **3320** through VPN communication link **3321** based on the VPN resources allocated by VPN gatekeeper **3314**. At step **3412**, web browser **3306** displays a secure icon indicating that the current communication link to server **3320** is a secure VPN communication link. Further communication between computers **3301** and **3320** occurs via the VPN, e.g., using a "hopping" regime as discussed above. When VPN link **3321** is terminated at step **3413**, flow continues to step **3414** where software module **3309** automatically replaces the secure top-level domain name with the corresponding non-secure top-level domain name for server **3304**. Browser **3306** accesses a standard DNS **3325** for obtaining the non-secure URL for server **3304**. Browser **3306** then connects to server **3304** in a well-known manner. At step **3415**, browser **3306** displays the "go secure" hyperlink or icon for selecting a VPN communication link between terminal **3301** and server **3304**. By again displaying the "go secure" hyperlink, a user is informed that the current communication link is a non-secure, non-VPN communication link.

When software module **3309** is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network **3302** are secure communication links. Thus, anytime that a communication link is established, the link is a VPN link. Consequently, software module **3309** transparently accesses SDNS **3313** for obtaining the URL for a selected secure website. In other words, in one embodiment, the user need not "click" on the secure option each time secure communication is to be effected.

Additionally, a user at computer **3301** can optionally select a secure communication link through proxy computer **3315**. Accordingly, computer **3301** can establish a VPN communication link **3323** with secure server computer **3320** through proxy computer **3315**. Alternatively, computer **3301** can establish a non-VPN communication link **3324** to a non-secure website, such as non-secure server computer **3304**.

FIG. **35** shows a flow diagram **3500** for registering a secure domain name according to the present invention. At step **3501**, a requester accesses website **3308** and logs into a secure domain name registry service that is available through website **3308**. At step **3502**, the requestor completes an online registration form for registering a secure domain name having a top-level domain name, such as .com, .net, .org, .edu, .mil or .gov. Of course, other secure top-level domain names can also be used. Preferably, the requestor must have previously registered a non-secure domain name corresponding to the equivalent secure domain name that is being requested. For example, a requestor attempting to register secure domain name "website.scom" must have previously registered the corresponding non-secure domain name "website.com".

At step **3503**, the secure domain name registry service at website **3308** queries a non-secure domain name server database, such as standard DNS **3322**, using, for example, a whois query, for determining ownership information relating to the non-secure domain name corresponding to the requested secure domain name. At step **3504**, the secure domain name registry service at website **3308** receives a reply from standard DNS **3322** and at step **3505** determines whether there is conflicting ownership information for the corresponding non-secure domain name. If there is no conflicting ownership information, flow continues to step **3507**, otherwise flow continues to step **3506** where the requestor is informed of the conflicting ownership information. Flow returns to step **3502**.

When there is no conflicting ownership information at step **3505**, the secure domain name registry service (website **3308**) informs the requester that there is no conflicting ownership information and prompts the requestor to verify the information entered into the online form and select an approved form of payment. After confirmation of the entered information and appropriate payment information, flow continues to step **3508** where the newly registered secure domain name sent to SDNS **3313** over communication link **3326**.

If, at step **3505**, the requested secure domain name does not have a corresponding equivalent non-secure domain name, the present invention informs the requestor of the situation and prompts the requestor for acquiring the corresponding equivalent non-secure domain name for an increased fee. By accepting the offer, the present invention automatically registers the corresponding equivalent non-secure domain name with standard DNS **3325** in a well-known manner. Flow then continues to step **3508**.

G. Tunneling Secure Address Hopping Protocol through Existing Protocol Using Web Proxy

The present invention also provides a technique for implementing the field hopping schemes described above in an application program on the client side of a firewall between two computer networks, and in the network stack on the server side of the firewall. The present invention uses a new secure connectionless protocol that provides good denial of service rejection capabilities by layering the new protocol on top of an existing IP protocol, such as the ICMP, UDP or TCP protocols. Thus, this aspect of the present invention does not require changes in the Internet infrastructure.

According to the invention, communications are protected by a client-side proxy application program that accepts unencrypted, unprotected communication packets from a local browser application. The client-side proxy application program tunnels the unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side. Of course, the unencrypted, unprotected communication packets can be encrypted prior to tunneling.

The client-side proxy application program is not an operating system extension and does not involve any modifications to the operating system network stack and drivers. Consequently, the client is easier to install, remove and support in comparison to a VPN. Moreover, the client-side proxy application can be allowed through a corporate firewall using a much smaller "hole" in the firewall and is less of a security risk in comparison to allowing a protocol layer VPN through a corporate firewall.

The server-side implementation of the present invention authenticates valid field-hopped packets as valid or invalid very early in the server packet processing, similar to a standard virtual private network, for greatly minimizing the impact of a denial of service attempt in comparison to normal TCP/IP and HTTP communications, thereby protecting the server from invalid communications.

FIG. **36** shows a system block diagram of a computer network **3600** in which a virtual private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks. FIG. **37** shows a flow diagram **3700** for establishing a virtual private connection that is encapsulated using an existing network protocol.

In FIG. **36** a local area network (LAN) **3601** is connected to another computer network **3602**, such as the Internet, through a firewall arrangement **3603**. Firewall arrangement operates in a well-known manner to interface LAN **3601** to computer network **3602** and to protect LAN **3601** from attacks initiated outside of LAN **3601**.

A client computer **3604** is connected to LAN **3601** in a well-known manner. Client computer **3604** includes an operating system **3605** and a web browser **3606**. Operating system **3605** provides kernel mode functions for operating client computer **3604**. Browser **3606** is an application program for accessing computer network resources connected to LAN **3601** and computer network **3602** in a well-known manner. According to the present invention, a proxy application **3607** is also stored on client computer **3604** and operates at an application layer in conjunction with browser **3606**. Proxy application **3607** operates at the application layer within client computer **3604** and when enabled, modifies unprotected, unencrypted message packets generated by browser **3606** by inserting data into the message packets that are used for forming a virtual private connection between client computer **3604** and a server computer connected to LAN **3601** or computer network **3602**. According to the invention, a virtual private connection does not provide the same level of security to the client computer as a virtual private network. A virtual private connection can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service that can be subscribed to by a user.

Proxy application **3607** is conveniently installed and uninstalled by a user because proxy application **3607** operates at the application layer within client computer **3604**. On installation, proxy application **3607** preferably configures browser **3606** to use proxy application for all web communications. That is, the payload portion of all message packets is modified with the data for forming a virtual private connection between client computer **3604** and a server computer. Preferably, the data for forming the virtual private connection contains field-hopping data, such as described above in connection with VPNs. Also, the modified message packets preferably conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol. Alternatively, proxy application **3606** can be selected and enabled through, for example, an option provided by browser **3606**. Additionally, proxy application **3607** can be enabled so that only the payload portion of specially designated message packets is modified with the data for forming a virtual private connection between client computer **3604** and a designated host computer. Specially designated message packets can be, for example, selected predetermined domain names.

Referring to FIG. **37**, at step **3701**, unprotected and unencrypted message packets are generated by browser **3606**. At step **3702**, proxy application **3607** modifies the payload portion of all message packets by tunneling the data for forming a virtual private connection between client computer **3604** and a destination server computer into the payload portion. At step, **3703**, the modified message packets are sent from client computer **3604** to, for example, website (server computer) **3608** over computer network **3602**.

Website **3608** includes a VPN guard portion **3609**, a server proxy portion **3610** and a web server portion **3611**. VPN guard portion **3609** is embedded within the kernel layer of the operating system of website **3608** so that large bandwidth attacks on website **3608** are rapidly rejected. When client computer **3604** initiates an authenticated connection to website **3608**, VPN guard portion **3609** is keyed with the hopping sequence contained in the message packets from client computer **3604**, thereby performing a strong authentication of the client packet streams entering website **3608** at step **3704**. VPN guard portion **3609** can be configured for providing different levels of authentication and, hence, quality of service, depending upon a subscribed level of service. That is, VPN guard portion **3609** can be configured to let all message packets through until a denial of service attack is detected, in which case VPN guard portion **3609** would allow only client packet streams conforming to a keyed hopping sequence, such as that of the present invention.

Server proxy portion **3610** also operates at the kernel layer within website **3608** and catches incoming message packets from client computer **3604** at the VPN level. At step **3705**, server proxy portion **3610** authenticates the message packets at the kernel level within host computer **3604** using the destination IP address, UDP ports and discriminator fields. The authenticated message packets are then forwarded to the authenticated message packets to web server portion **3611** as normal TCP web transactions.

At step **3705**, web server portion **3611** responds to message packets received from client computer **3604** in accordance with the particular nature of the message packets by generating reply message packets. For example, when a client computer requests a webpage, web server portion **3611** generates message packets corresponding to the requested webpage. At step **3706**, the reply message packets pass through server proxy portion **3610**, which inserts data into the payload portion of the message packets that are used for forming the virtual private connection between host computer **3608** and client computer **3604** over computer network **3602**. Preferably, the data for forming the virtual private connection is contains field-hopping data, such as described above in connection with VPNs. Server proxy portion **3610** operates at the kernel layer within host computer **3608** to insert the virtual private connection data into the payload portion of the reply message packets. Preferably, the modified message packets sent by host computer **3608** to client computer **3604** conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol.

At step **3707**, the modified packets are sent from host computer **3608** over computer network **3602** and pass through firewall **3603**. Once through firewall **3603**, the modified packets are directed to client computer **3604** over LAN **3601** and are received at step **3708** by proxy application **3607** at the application layer within client computer **3604**. Proxy application **3607** operates to rapidly evaluate the modified message packets for determining whether the received packets should be accepted or dropped. If the virtual private connection data inserted into the received information packets conforms to expected virtual private connection data, then the received packets are accepted. Otherwise, the received packets are dropped.

While the present invention has been described in connection with the illustrated embodiments, it will be appreciated and understood that modifications may be made without departing from the true spirit and scope of the invention.

What is claimed is:

1. A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising:

receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device; and

sending a message over a secure communication link from the first device to the second device.

2. A method of using a first device to communicate with a second device having a secure name, the method comprising:

from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;

at the first device, receiving a message containing the network address associated with the secure name of the second device; and

from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

3. The method according to claim **2**, wherein the secure name of the second device is a secure domain name.

4. The method according to claim **2**, wherein the secure name indicates security.

5. The method according to claim **2**, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.

6. The method according to claim **5**, further including decrypting the message.

7. The method according to claim **2**, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.

8. The method according to claim **2**, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device.

9. The method according to claim **2**, further including automatically initiating the secure communication link after it is enabled.

10. The method according to claim **2**, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.

11. The method according to claim **2**, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.

12. The method according to claim **2**, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols.

13. The method according to claim **2**, wherein the receiving and sending of messages through the secure communication link includes multiple sessions.

14. The method according to claim **2**, further including supporting a plurality of services over the secure communication link.

15. The method according to claim **14**, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

16. The method according to claim **15**, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.

17. The method according to claim **15**, wherein the plurality of services comprises audio, video or a combination thereof.

18. The method according to claim **2**, wherein the secure communication link is an authenticated link.

19. The method according to claim **2**, wherein the first device is a computer, and the steps are performed on the computer.

20. The method according to claim **2**, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.

21. The method according to claim **2**, further including providing an unsecured name associated with the device.

22. The method according to claim **2**, wherein the secure name is registered prior to the step of sending a message to a secure name service.

23. The method according to claim **2**, wherein the secure name of the second device is a secure, non-standard domain name.

24. A method of using a first device to securely communicate with a second device over a communication network, the method comprising:

at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;

receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and

sending a message securely from the first device to the second device.

25. The method according to claim **24**, wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.

26. A method of using a first device to communicate with a second device over a communication network, the method comprising:

from the first device requesting and obtaining registration of an unsecured name associated with the first device;

from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;

receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

from the first device sending a message securely from the first device to the second device.

27. The method according to claim **26**,

wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and

wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.

28. A non-transitory machine-readable medium comprising instructions for:

sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

receiving a message containing the network address associated with the secure name of the device; and

sending a message to the network address associated with the secure name of the device using a secure communication link.

29. A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and

sending a message securely from the first device to the second device.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO.	: 8,051,181 B2
APPLICATION NO.	: 11/679416
DATED	: November 1, 2011
INVENTOR(S)	: Victor Larson et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the cover of the patent: Amend item (60), first paragraph, under the heading "Related U.S. Application Data," as follows:

Delete item (60), first paragraph, and insert the following paragraph:

--Continuation of application No. 10/702,486, filed on Nov. 7, 2003, now Pat. No. 7,188,180, which is a division of application No. 09/558,209, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.--

Signed and Sealed this
Third Day of January, 2012

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

Substitute for form PTO/SB/42

INFORMATION DISCLOSURE STATEMENT BY REQUESTOR

Complete if Known	
Docket Number	41484-80200
Application/Control No.	
Confirmation No.	
Examiner	
Group Art Unit	
Patent No. under Reexamination	8,051,181
Inventor	Larson et al.
Issue Date	November 1, 2011

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite #	DOCUMENT NUMBER	CODE	NAME	ISSUE DATE (mm/dd/yyyy)	CLASS	SUB CLASS	Filing Date if Appropriate
	X2	6131121	A	Mattaway et al	10/10/2000	709	227	
	X1	6496867	B1	Beser et al.	12/17/2002	709	245	
	X6	6499108	B1	Johnson, R.	12/24/2002	713	201	
	X4	6557037	B1	Provino, J.	04/29/2003	709	227	

OTHER DOCUMENTS

Examiner Initials	Cite #	Include Author, Title, Date, Pertinent Pages, etc.
	X3	Lendenmann, R. et al., "Understanding OSF DCE 1.1 for AIX and OS/2," IBM Corporation International Technical Support Organization (October 1995); pp. 1-274.
	X5	Droms, R. RFC 2131, "Dynamic Host Configuration Protocol" (November 1987); pp. 1-39.
	X7	ITU-T Recommendation H.323, "Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services. Packet-based multimedia communications systems," International Telecommunications Union (February 1998); pp. 1-128.
	X8	ITU-T Recommendation H.225.0, "Infrastructure of audiovisual services – Transmission multiplexing and synchronization. Call signalling protocols and media stream packetization for packet-based multimedia communication systems," International Telecommunication Union (February 1998); pp. 1-155.
	X9	ITU-T Recommendation H.235, "Infrastructure of audiovisual services – Systems aspects. Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," International Telecommunication Union (February 1998); pp. 1-39.
	X10	ITU-T Recommendation H.245, "Infrastructure of audiovisual services – Communication procedures. Control protocol for multimedia communication," International Telecommunication Union (February 1998); pp. 1-280.
	X11	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities" (November 1987); pp. 1-47.

Examiner Signature		Date Considered	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Also referred to as FORM PTO-1465)

REQUEST FOR *INTER PARTES* REEXAMINATION TRANSMITTAL FORM

Address to:
Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attorney Docket No.: 41484-80200

Date: March 28, 2012

1. ☒ This is a request for *inter partes* reexamination pursuant to 37 CFR 1.913 of patent number 8,051,181 issued November 1, 2011. The request is made by a third party requester, identified herein below.

2. ☒ a. The name and address of the person requesting reexamination is:
Jeffrey P. Kushan
Sidley Austin LLP
1501 K Street, N.W. Washington, D.C., 20005

b. The real party in interest (37 CFR 1.915(b)(8)) is: Apple Inc., 1 Infinite Loop, Cupertino CA95014

3. ☐ a. A check in the amount of $__________ is enclosed to cover the reexamination fee, 37 CFR 1.20(c)(2);

☒ b. The Director is hereby authorized to charge the fee as set forth in 37 CFR 1.20(c)(2) to Deposit Account No. 18-1260 ; **or**

☐ c. Payment by credit card. Form PTO-2038 is attached.

4. ☒ Any refund should be made by ☐ check or ☒ credit to Deposit Account No. 18-1260
37 CFR 1.26(c). If payment is made by credit card, refund must be to credit card account.

5. ☒ A copy of the patent to be reexamined having a double column format on one side of a separate paper is enclosed. 37 CFR 1.915(b)(5)

6. ☐ CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table
☐ Landscape Table on CD

7. ☐ Nucleotide and/or Amino Acid Sequence Submission
If applicable, items a. – c. are required.

a. ☐ Computer Readable Form (CRF)

b. Specification Sequence Listing on:

i. ☐ CD-ROM (2 copies) or CD-R (2 copies); **or**

ii. ☐ paper

c. ☐ Statements verifying identity of above copies

8. ☒ A copy of any disclaimer, certificate of correction or reexamination certificate issued in the patent is included.

9. ☒ Reexamination of claim(s) 1 - 29 is requested.

10. ☒ A copy of every patent or printed publication relied upon is submitted herewith including a listing thereof on Form PTO/SB/08, PTO-1449, or equivalent.

11. ☐ An English language translation of all necessary and pertinent non-English language patents and/or printed publications is included.

This collection of information is required by 37 CFR 1.915. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop *Inter Partes* Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

12. ☒ The attached detailed request includes at least the following items:

a. A statement identifying each substantial new question of patentability based on prior patents and printed publications. 37 CFR 1.915(b)(3)
b. An identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited art to every claim for which reexamination is requested. 37 CFR 1.915(b)(1) & (3).

13. ☒ It is certified that the estoppel provisions of 37 CFR 1.907 do not prohibit this reexamination. 37 CFR 1.915(b)(7)

14. ☒ a. It is certified that a copy of this request has been served in its entirety on the patent owner as provided in 37 CFR 1.33(c).
The name and address of the party served and the date of service are:

VirnetX Inc.
c/o McDermott Will & Emery
600 13th Street, N.W. Washington, D.C. 20005-3096

Date of Service: March 28, 2012; **or**

□ b. A duplicate copy is enclosed because service on patent owner was not possible. An explanation of the efforts made to serve patent owner **is attached**. See MPEP 2620.

15. Third Party Requester Correspondence Address: Direct all communications about the reexamination to:

☒ The address associated with Customer Number: 26116

OR

□ Firm or Individual Name

Address

City

State

Zip

Country

Telephone

Email

16. ☒ The patent is currently the subject of the following concurrent proceeding(s):

□ a. Copending reissue Application No.
□ b. Copending reexamination Control No.
□ c. Copending Interference No.
☒ d. Copending litigation styled:
VirnetX Inc. v. Cisco Systems, Inc., Apple, Inc., et al.,
Civ. Act. No. 6:10-cv-417 (E.D. Tex.)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

/Jeffrey P. Kushan/Reg. No. 43,401
Authorized Signature

March 28, 2012
Date

Jeffrey P. Kushan
Typed/Printed Name

43,401
Registration No., if applicable

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 4522

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
95/001,949	03/28/2012 RULE	709	3992	41484-80200

APPLICANTS

8051181, Residence Not Provided;
VIRNETX INC.(OWNER), ZEPHYR COVE, NV;
JEFFREY P. KUSHAN(3RD.PTY.REQ.), WASHINGTON, DC;
APPLE INC.,(REAL PTY IN INTEREST), CUPERTINO, CA;
SIDLEY AUSTIN LLP, DALLAS, TX

** CONTINUING DATA *************************

This application is a REX of 11/679,416 02/27/2007 PAT 8051181
which is a CON of 10/702,486 11/07/2003 PAT 7188180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6502135
which is a CIP of 09/429,643 10/29/1999 PAT 7010604
which claims benefit of 60/106,261 10/30/1998

** FOREIGN APPLICATIONS ********************

		STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed	□ yes □ no				
35 USC 119 (a-d) conditions met	□ yes □ no □ Met after Allowance				
Verified and Acknowledged	Examiner's Signature Initials				

ADDRESS
23630

TITLE
METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _________ to charge/credit DEPOSIT ACCOUNT No. _________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue) □ Other ______________ □ Credit

Litigation Search Report CRU 3999

Reexam Control No. 95/001,949

To: Examiner	From: Alicia Kelley-Collier
Location: CRU	Location: CRU 3999
Art Unit: 3999	MDE 5A74
Date: 4/6/12	Phone: (571) 272-6059
Case Serial Number: 95/001,949	alicia.kelley@uspto.gov

Search Notes

U.S. Patent No. **8,051,181**

1) I performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.

2) I performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.

3) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.

4) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.

5) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Litigation was found for this Patent:

6:11cv563 **Open** **12/07/2011** - Unopposed MOTION to Stay OF PROCEEDINGS PURSUANT TO 28 U.S.C. &#167

12/15/2011 - ORDER granting 7 Motion to Stay. This civil action is STAYED until the determination of the International Trade Commission in Investigation No. 337-TA-818 becomes final.

Date of Printing: Apr 06, 2012

KEYCITE

C US PAT 8051181 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, Assignee: Virnetx, Inc. (Nov 01, 2011)

History

Direct History

=> 1 **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK,** US PAT 8051181 (U.S. PTO Utility Nov 01, 2011)

Patent Family

2 INFORMATION TRANSMISSION INVOLVES COMPARING DISCRIMINATOR VALUE FOR EACH RECEIVED DATA PACKET WITH SET OF VALID DISCRIMINATOR VALUES, ACCEPTING RECEIVED DATA PACKET FOR FURTHER PROCESSING WHILE DETECTING MATCH, Derwent World Patents Legal 2000-399393+

Assignments

3 Action: CHANGE OF ADDRESS OF ASSIGNEE Number of Pages: 003, (DATE RECORDED: Jan 19, 2012)

4 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS). Number of Pages: 004, (DATE RECORDED: Jun 21, 2007)

5 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS). Number of Pages: 006, (DATE RECORDED: Jun 21, 2007)

Patent Status Files

.. Certificate of Correction, (OG DATE: Jan 24, 2012)

.. Patent Suit(See LitAlert Entries),

Docket Summaries

8 VIRNETX INC. v. APPLE INC, (E.D.TEX. Nov 01, 2011) (NO. 6:11CV00563), (35 USC 271)

Litigation Alert

9 Derwent LitAlert P2011-46-19 (Nov 01, 2011) Action Taken: cause - 35 USC 271 - COMPLAINT FOR PATENT INFRINGEMENT

Prior Art (Coverage Begins 1976)

C 10 ACCESS CONTROL OF NETWORKED DATA, US PAT 6233618Assignee: Content Advisor, Inc., (U.S. PTO Utility 2001)

C 11 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, US PAT APP 20080040792Assignee: VirnetX, Inc., (U.S. PTO Application 2008)

C 12 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, US PAT APP 20080040783Assignee: VirnetX, Inc., (U.S. PTO Application 2008)

C 13 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, US PAT APP 20040098485Assignee: Science Applications International, (U.S. PTO Application 2004)

C 14 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20080222415Assignee: VirnetX, Inc., (U.S. PTO Application 2008)

C 15 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20080040791Assignee: VirnetX, Inc., (U.S. PTO Application 2008)

C 16 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20080034201Assignee: VirnetX, Inc., (U.S. PTO Application 2008)

C 17 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 7133930Assignee: Science Applications International, (U.S. PTO Utility 2006)

C 18 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20060123134Assignee: Science Applications International, (U.S. PTO Application 2006)

C 19 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 7010604Assignee: Science Applications International, (U.S. PTO Utility 2006)

C 20 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20040003116Assignee: Science Applications International, (U.S. PTO Application 2004)

C 21 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6618761Assignee: Science Applications International Corp., (U.S. PTO Utility 2003)

C 22 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20030167342Assignee: Science Applications International, (U.S. PTO Application 2003)

C 23 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT APP 20030037142Assignee: Science Applications International, (U.S. PTO Application 2003)

H 24 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED

SYSTEM AVAILABILITY, US PAT 6502135Assignee: Science Applications International, (U.S. PTO Utility 2002)

C 25 APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM, US PAT 5787172Assignee: The Merdan Group, Inc., (U.S. PTO Utility 1998)

C 26 APPARATUS AND METHOD FOR HYBRID NETWORK ACCESS, US PAT 6571296Assignee: Hughes Electronics Corporation, (U.S. PTO Utility 2003)

C 27 APPARATUS AND METHOD FOR WEB FORWARDING, US PAT 7461334Assignee: Network Solutions, LLC, (U.S. PTO Utility 2008)

C 28 APPARATUS FOR IMPLEMENTING VIRTUAL PRIVATE NETWORKS, US PAT 6173399Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2001)

C 29 APPARATUS FOR MAKING TWO COMPONENT FIBERS OR CONTINUOUS FILAMENTS USING FLEXIBLE TUBE INSERTS, US PAT 6168409 (U.S. PTO Utility 2001)

C 30 ARCHITECTURE FOR VIRTUAL PRIVATE NETWORKS, US PAT 6226748Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2001)

C 31 AUDIO-ACTIVE COMMUNICATION STATIONS, COMMUNICATION METHOD AND COMMUNICATION SYSTEM WITH AUDIO-ACTIVE COMMUNICATION STATIONS, US PAT 6687551Assignee: Siemens Aktiengesellschaft, (U.S. PTO Utility 2004)

C 32 AUTOCONFIGURABLE METHOD AND SYSTEM HAVING AUTOMATED DOWNLOADING, US PAT 5870610Assignee: Siemens Business Communication Systems,, (U.S. PTO Utility 1999)

C 33 AUTOMATIC PROCESS CONTROL SYSTEM, US PAT 2895502 (U.S. PTO Utility 1959)

C 34 CLOCK SYNCHRONIZATION SYSTEM AND METHOD USING A CONTINUOUS CONVERSION FUNCTION FOR A COMMUNICATION NETWORK, US PAT 6157957Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2000)

C 35 COMPUTER NETWORK SWITCHING SYSTEM WITH EXPANDABLE NUMBER OF PORTS, US PAT 5561669Assignee: Cisco Systems, Inc., (U.S. PTO Utility 1996)

C 36 CONGESTION AVOIDANCE ON COMMUNICATIONS NETWORKS, US PAT 6430155Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2002)

C 37 CRYPTOGRAPHIC KEY MANAGEMENT APPARATUS AND METHOD, US PAT 5341426Assignee: Motorola, Inc., (U.S. PTO Utility 1994)

C 38 DATA ENCLAVE AND TRUSTED PATH SYSTEM, US PAT 5276735Assignee: Secure Computing Corporation, (U.S. PTO Utility 1994)

C 39 DATA TRANSMISSION METHOD AND DEVICE, US PAT 6760766 (U.S. PTO Utility 2004)

C 40 DIGITAL IDENTITY REGISTRATION, US PAT APP 20070208869Assignee: THE GO DADDY GROUP, INC., (U.S. PTO Application 2007)

C 41 DOMAIN NAME MANAGEMENT SYSTEM AND METHOD, US PAT APP 20070214284Assignee: SnapNames.com, Inc., (U.S. PTO Application 2007)

C 42 DOMAIN NAME OWNERSHIP VALIDATION, US PAT 7493403Assignee: Markmonitor Inc., (U.S. PTO Utility 2009)

C 43 DOMAIN NAME ROUTING, US PAT 6119171Assignee: IP Dynamics, Inc., (U.S. PTO Utility

2000)

C 44 DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION, US PAT 6332158 (U.S. PTO Utility 2001)

C 45 DUAL MASTER IMPLIED TOKEN COMMUNICATION SYSTEM, US PAT 4988990Assignee: Rosemount Inc., (U.S. PTO Utility 1991)

C 46 DYNAMIC NETWORK ADDRESS UPDATING, US PAT 6243749Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2001)

C 47 DYNAMIC SELECTION OF NETWORK PROVIDERS, US PAT 6243754Assignee: International Business Machines, (U.S. PTO Utility 2001)

C 48 ENCRYPTED COMMUNICATION METHOD, US PAT APP 20080235507 (U.S. PTO Application 2008)

C 49 ENCRYPTED VIRTUAL TERMINAL EQUIPMENT HAVING INITIALIZATION DEVICE FOR PREVENTING REPLY ATTACK, US PAT 5384848Assignee: Fujitsu Limited, (U.S. PTO Utility 1995)

C 50 ENHANCED DOMAIN NAME SERVICE USING A MOST FREQUENTLY USED DOMAIN NAMES TABLE AND A VALIDITY CODE TABLE, US PAT 6016512Assignee: Telcordia Technologies, Inc., (U.S. PTO Utility 2000)

C 51 ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST, US PAT 7490151Assignee: Virnetx Inc., (U.S. PTO Utility 2009)

C 52 FAST NETWORK LAYER PACKET FILTER, US PAT 6147976Assignee: Cabletron Systems, Inc., (U.S. PTO Utility 2000)

C 53 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6751738 (U.S. PTO Utility 2004)

C 54 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT APP 20030196122 (U.S. PTO Application 2003)

C 55 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6052788Assignee: Network Engineering Software, Inc., (U.S. PTO Utility 2000)

C 56 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 5898830Assignee: Network Engineering Software, (U.S. PTO Utility 1999)

C 57 FORWARDING INTERNETWORK PACKETS BY REPLACING THE DESTINATION ADDRESS, US PAT 5740375Assignee: Bay Networks, Inc., (U.S. PTO Utility 1998)

C 58 FORWARDING OF INTERNETWORK PACKETS TO A DESTINATION NETWORK VIA A SELECTED ONE OF A PLURALITY OF PATHS, US PAT 5845091Assignee: Bay Networks, Inc., (U.S. PTO Utility 1998)

C 59 GAS DISTRIBUTION APPARATUS FOR SEMICONDUCTOR PROCESSING, US PAT 6333272Assignee: Lam Research Corporation, (U.S. PTO Utility 2001)

C 60 GENERALIZED SECURITY POLICY MANAGEMENT SYSTEM AND METHOD, US PAT 5950195Assignee: Secure Computing Corporation, (U.S. PTO Utility 1999)

C 61 GENERIC HIGH BANDWIDTH ADAPTER HAVING DATA PACKET MEMORY CONFIGURED IN THREE LEVEL HIERARCHY FOR TEMPORARY STORAGE OF VARIABLE LENGTH DATA PACKETS, US PAT 5367643Assignee: International Business Machines, (U.S. PTO Utility 1994)

C 62 INTERMEDIATE NETWORK AUTHENTICATION, US PAT 5511122Assignee: The United States of America as, (U.S. PTO Utility 1996)

C 63 LEAST PRIVILEGE VIA RESTRICTED TOKENS, US PAT 6308274Assignee: Microsoft Corporation, (U.S. PTO Utility 2001)

C 64 LOW TRAFFIC NETWORK MANAGEMENT METHOD USING ESTIMATED PROCESS EXECUTION TIME FOR MANAGER-AGENT SYNCHRONIZATION, US PAT 6041342Assignee: NEC Corporation, (U.S. PTO Utility 2000)

C 65 MAINTAINING PACKET SECURITY IN A COMPUTER NETWORK, US PAT 6571338Assignee: Sun Microsystems Inc., (U.S. PTO Utility 2003)

C 66 MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS, US PAT 5905859Assignee: International Business Machines, (U.S. PTO Utility 1999)

C 67 MANAGING USER INFORMATION ON AN E- COMMERCE SYSTEM, US PAT 7100195Assignee: Accenture LLP, (U.S. PTO Utility 2006)

C 68 METHOD AND APPARATUS FOR AUTHENTICATING CONNECTIONS TO A STORAGE SYSTEM COUPLED TO A NETWORK, US PAT 6263445Assignee: EMC Corporation, (U.S. PTO Utility 2001)

C 69 METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION, US PAT 5796942Assignee: Computer Associates International, Inc., (U.S. PTO Utility 1998)

C 70 METHOD AND APPARATUS FOR CLIENT-HOST COMMUNICATION OVER A COMPUTER NETWORK, US PAT 6119234Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 2000)

C 71 METHOD AND APPARATUS FOR CONFIGURING A VIRTUAL PRIVATE NETWORK, US PAT 6226751Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2001)

C 72 METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM, US PAT 5892903Assignee: Internet Security Systems, Inc., (U.S. PTO Utility 1999)

C 73 METHOD AND APPARATUS FOR DNS RESOLUTION, US PAT 6425003Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2002)

C 74 METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM, US PAT 6006259Assignee: Network Alchemy, Inc., (U.S. PTO Utility 1999)

C 75 METHOD AND APPARATUS FOR A KEY-MANAGEMENT SCHEME FOR INTERNET PROTOCOLS, US PAT 5588060Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1996)

C 76 METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK, US PAT 6079020Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2000)

C 77 METHOD AND APPARATUS FOR MODIFYING A TRANSPORT PACKET STREAM TO PROVIDE CONCATENATED SYNCHRONIZATION BYTES AT INTERLEAVER OUTPUT, US PAT 5771239Assignee: General Instrument Corporation of Delaware, (U.S. PTO Utility 1998)

C 78 METHOD AND APPARATUS FOR PREVENTING MISROUTING OF DATA IN A RADIO COMMUNICATION SYSTEM, US PAT 6246670Assignee: Telefonaktiebolaget L M Ericsson (Publ), (U.S. PTO Utility 2001)

C 79 METHOD AND APPARATUS FOR PROCESSING COMMUNICATIONS IN A VIRTUAL PRIVATE NETWORK, US PAT 6701437Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2004)

C 80 METHOD AND APPARATUS FOR PROVIDING A DETERMINED RATIO OF PROCESS FLUIDS, US PAT 6752166Assignee: Celerity Group, Inc., (U.S. PTO Utility 2004)

C 81 METHOD AND APPARATUS FOR PROVIDING NETWORK ACCESS CONTROL USING A DOMAIN NAME SYSTEM, US PAT 6256671Assignee: Nortel Networks Limited, (U.S. PTO Utility 2001)

C 82 METHOD AND APPARATUS FOR PROVIDING A VIRTUAL PRIVATE NETWORK, US PAT 6092200Assignee: Novell, Inc., (U.S. PTO Utility 2000)

C 83 METHOD AND APPARATUS FOR REDUNDANT LOCAL AREA NETWORK SYSTEMS, US PAT 5329521 (U.S. PTO Utility 1994)

C 84 METHOD AND APPARATUS FOR SECURE DATA PACKET BUS COMMUNICATION, US PAT 5559883Assignee: Chipcom Corporation, (U.S. PTO Utility 1996)

C 85 METHOD AND APPARATUS FOR SYNCHRONIZATION OF TWO COMPUTER SYSTEMS BY EXECUTING A SYNCHRONIZATION PROCESS AT A PORTABLE COMPUTER, US PAT 6671702Assignee: PalmSource, Inc., (U.S. PTO Utility 2003)

C 86 METHOD AND PROTOCOL FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION, US PAT 6353614Assignee: 3Com Corporation, (U.S. PTO Utility 2002)

C 87 METHOD AND PROTOCOL FOR SYNCHRONIZED TRANSFER-WINDOW BASED FIREWALL TRAVERSAL, US PAT 6202081Assignee: 3Com Corporation, (U.S. PTO Utility 2001)

C 88 METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES, US PAT 6286047Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)

C 89 METHOD AND SYSTEM FOR BALANCING LOAD DISTRIBUTION ON A WIDE AREA NETWORK, US PAT APP 20010049741 (U.S. PTO Application 2001)

C 90 METHOD AND SYSTEM FOR COMMUNICATING BETWEEN CLIENTS IN A COMPUTER NETWORK, US PAT 7188175Assignee: Web.com, Inc., (U.S. PTO Utility 2007)

C 91 METHOD AND SYSTEM FOR MEASURING QUEUE LENGTH AND DELAY, US PAT 6314463Assignee: WebSpective Software, Inc., (U.S. PTO Utility 2001)

C 92 METHOD FOR CHECKING THE AVAILABILITY OF A DOMAIN NAME, US PAT APP 20040199520Assignee: Parsons Advanced Holdings, Inc., (U.S. PTO Application 2004)

C 93 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT APP 20080216168Assignee: VirnetX, Inc., (U.S. PTO Application 2008)

H 94 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT 7188180Assignee: VimetX, Inc., (U.S.

PTO Utility 2007)

C 95 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT 6826616Assignee: Science Applications International Corp., (U.S. PTO Utility 2004)

C 96 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT APP 20040107285Assignee: Science Applications International, (U.S. PTO Application 2004)

C 97 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT APP 20040103205Assignee: Science Applications International, (U.S. PTO Application 2004)

H 98 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK WITHOUT USER ENTERING ANY CRYPTOGRAPHIC INFORMATION, US PAT 6839759Assignee: Science Applications International Corp., (U.S. PTO Utility 2005)

C 99 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK WITHOUT USER ENTERING ANY CRYPTOGRAPHIC INFORMATION, US PAT APP 20040107286Assignee: Science Applications International, (U.S. PTO Application 2004)

C 100 METHOD FOR ESTABLISHING A SECURED COMMUNICATION CHANNEL OVER THE INTERNET, US PAT 6223287Assignee: International Business Machines, (U.S. PTO Utility 2001)

C 101 METHOD FOR GATHERING DOMAIN NAME REGISTRATION INFORMATION FROM A REGISTRANT VIA A REGISTRAR&apos;S WEB SITE, US PAT APP 20040199608 (U.S. PTO Application 2004)

C 102 METHOD FOR NETWORK ADDRESS TRANSLATION, US PAT 6006272Assignee: Lucent Technologies Inc., (U.S. PTO Utility 1999)

C 103 METHOD FOR REGISTERING A STREAM OF DOMAIN NAMES RECEIVED VIA A REGISTRAR&apos;S WEB SITE, US PAT APP 20040199493 (U.S. PTO Application 2004)

C 104 METHOD FOR TRANSFERING A REGISTERED DOMAIN NAME FROM A FIRST REGISTRAR TO A SECOND REGISTRAR, US PAT APP 20040199620 (U.S. PTO Application 2004)

C 105 METHOD OF AND SYSTEM FOR EXTENDING INTERNET TELEPHONY OVER VIRTUAL PRIVATE NETWORK DIRECT ACCESS LINES, US PAT 6453034Assignee: MCI WorldCom, Inc., (U.S. PTO Utility 2002)

C 106 METHOD OF AUTOMATICALLY DETERMINING A TRANSMISSION ORDER OF PACKET IN A LOCAL AREA NETWORK AND APPARATUS FOR SAME, US PAT 5625626Assignee: Hitachi, Ltd., (U.S. PTO Utility 1997)

C 107 METHOD OF PROVIDING A SERVICE THROUGH A SERVER WITH A VIRTUAL SINGLE NETWORK ADDRESS, US PAT 6055574Assignee: Unisys Corporation, (U.S. PTO Utility 2000)

C 108 METHOD OF USING ELECTRONIC TICKETS CONTAINING PRIVILEGES FOR IMPROVED SECURITY, US PAT 6505232Assignee: WebTV Networks, Inc., (U.S. PTO Utility 2003)

C 109 METHOD OF USING ELECTRONIC TICKETS CONTAINING PRIVILEGES FOR IMPROVED SECURITY, US PAT 6311207Assignee: WebTV Networks, Inc., (U.S. PTO Utility 2001)

C 110 METHOD OF USING ROUTING PROTOCOLS TO REROUTE PACKETS DURING A LINK FAILURE, US PAT 6301223Assignee: Scientific-Atlanta, Inc., (U.S. PTO Utility 2001)

C 111 METHOD, PRODUCT, AND APPARATUS FOR REQUESTING A NETWORK RESOURCE, US PAT 6338082 (U.S. PTO Utility 2002)

C 112 METHOD TO ESTABLISH AND ENFORCE A NETWORK CRYPTOGRAPHIC SECURITY POLICY IN A PUBLIC KEY CRYPTOSYSTEM, US PAT 5164988Assignee: International Business Machines, (U.S. PTO Utility 1992)

C 113 MODE OF HANTJFACTTM$#amp;NE WOOL OK OTHBB FIBBOTJS MATERIALS.", US PAT 2 (U.S. PTO Utility 1836)

H 114 MULTI-ACCESS VIRTUAL PRIVATE NETWORK, US PAT 6158011Assignee: V-One Corporation, (U.S. PTO Utility 2000)

C 115 MULTI-FUNCTION NETWORK, US PAT 5654695Assignee: International Business Machines, (U.S. PTO Utility 1997)

C 116 MULTIPLE NETWORK CONFIGURATION WITH LOCAL AND REMOTE NETWORK REDUNDANCY BY DUAL MEDIA REDIRECT, US PAT 6324161Assignee: Alcatel USA Sourcing, L.P., (U.S. PTO Utility 2001)

C 117 MULTIPROCESSOR/MEMORY INTERCONNECTION NETWORK WHEREIN MESSAGES SENT THROUGH THE NETWORK TO THE SAME MEMORY ARE COMBINED, US PAT 4920484Assignee: Yale University, (U.S. PTO Utility 1990)

C 118 NETWORK COMMUNICATIONS ADAPTER WITH DUAL INTERLEAVED MEMORY BANKS SERVICING MULTIPLE PROCESSORS, US PAT 4933846Assignee: Network Systems Corporation, (U.S. PTO Utility 1990)

C 119 NETWORK FAULT DETECTION AND RECOVERY, US PAT 6581166Assignee: The Foxboro Company, (U.S. PTO Utility 2003)

C 120 NETWORK PACKET RECEIVER WITH BUFFER LOGIC FOR REASSEMBLING INTERLEAVED DATA PACKETS, US PAT 5303302Assignee: Digital Equipment Corporation, (U.S. PTO Utility 1994)

C 121 NETWORK SERVER HAVING DYNAMIC LOAD BALANCING OF MESSAGES IN BOTH INBOUND AND OUTBOUND DIRECTIONS, US PAT 6243360Assignee: International Business Machines, (U.S. PTO Utility 2001)

C 122 NETWORK STATION WITH MULTIPLE NETWORK ADDRESSES, US PAT 5590285Assignee: 3Com Corporation, (U.S. PTO Utility 1996)

C 123 NETWORK WITH SECURE COMMUNICATIONS SESSIONS, US PAT 5689566 (U.S. PTO Utility 1997)

C 124 OUT-OF-BAND DATA TRANSMISSION, US PAT 5867650Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)

C 125 PARALLEL COMPUTER SYSTEM FOR PERFORMING BARRIER SYNCHRONIZATION BY TRANSFERRING THE SYNCHRONIZATION PACKET THROUGH A PATH WHICH

BYPASSES THE PACKET BUFFER IN RESPONSE TO AN INTERRUPT, US PAT 5682480Assignee: Hitachi, Ltd., (U.S. PTO Utility 1997)

H 126 POLICY CACHING METHOD AND APPARATUS FOR USE IN A COMMUNICATION DEVICE BASED ON CONTENTS OF ONE DATA UNIT IN A SUBSET OF RELATED DATA UNITS, US PAT 5842040Assignee: Storage Technology Corporation, (U.S. PTO Utility 1998)

C 127 PROCESSING TAXONOMIC EXTENSIONS ON THE WORLD WIDE WEB TO IMPLEMENT AN INTEGRITY- RICH INTELLIGENCE APPARATUS, US PAT APP 20070266141 (U.S. PTO Application 2007)

C 128 PROTECTING OPEN WORLD WIDE WEB SITES FROM KNOWN MALICIOUS USERS BY DIVERTING REQUESTS FROM MALICIOUS USERS TO ALIAS ADDRESSES FOR THE PROTECTED SITES, US PAT 6714970Assignee: International Business Machines, (U.S. PTO Utility 2004)

C 129 REINITIATION OF BIND CALLS FOR IP APPLICATIONS CONCURRENTLY EXECUTING WITH ALTERNATE ADDRESS, US PAT 5996016Assignee: International Business Machines, (U.S. PTO Utility 1999)

C 130 RELATIVE PRESSURE CONTROL SYSTEM AND RELATIVE FLOW CONTROL SYSTEM, US PAT 7353841Assignee: CKD Corporation; Tokyo Electron Limited, (U.S. PTO Utility 2008)

C 131 ROUTING OVER SIMILAR PATHS, US PAT 6061736Assignee: 3Com Corporation, (U.S. PTO Utility 2000)

C 132 SCHEME TO ALLOW TWO COMPUTERS ON A NETWORK TO UPGRADE FROM A NON-SECURED TO A SECURED SESSION, US PAT 5822434Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1998)

C 133 SECURE ACCESS METHOD, AND ASSOCIATED APPARATUS, FOR ACCESSING A PRIVATE IP NETWORK, US PAT 6061346Assignee: Telefonaktiebolaget LM Ericsson (publ), (U.S. PTO Utility 2000)

C 134 SECURE DELIVERY OF INFORMATION IN A NETWORK, US PAT 6178505Assignee: Internet Dynamics, Inc., (U.S. PTO Utility 2001)

C 135 SECURE INTRANET ACCESS, US PAT 6081900Assignee: Novell, Inc., (U.S. PTO Utility 2000)

C 136 SECURE SERVER ARCHITECTURE FOR WEB BASED DATA MANAGEMENT, US PAT 6606708Assignee: WorldCom, Inc., (U.S. PTO Utility 2003)

C 137 SECURE WEB TUNNEL, US PAT 5805803Assignee: Digital Equipment Corporation, (U.S. PTO Utility 1998)

C 138 SECURITY SYSTEM FOR NETWORK ADDRESS TRANSLATION SYSTEMS, US PAT 6510154Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2003)

C 139 SECURITY SYSTEM FOR A NETWORK CONCENTRATOR, US PAT 5311593Assignee: Chipcom Corporation, (U.S. PTO Utility 1994)

C 140 SENDING INSTRUCTIONS FROM A SERVICE MANAGER TO FORWARDING AGENTS ON A NEED TO KNOW BASIS, US PAT 6549516Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2003)

C 141 SIGNALING METHOD FOR INTERNET TELEPHONY, US PAT 6937597Assignee: Lucent

Technologies Inc., (U.S. PTO Utility 2005)

C 142 SYSTEM AND METHOD FOR ACHIEVING NETWORK SEPARATION, US PAT 5918018Assignee: Secure Computing Corporation, (U.S. PTO Utility 1999)

C 143 SYSTEM AND METHOD FOR DATA SECURITY, US PAT 5629984Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1997)

C 144 SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY, US PAT 5805801Assignee: International Business Machines, (U.S. PTO Utility 1998)

C 145 SYSTEM AND METHOD FOR EASING COMMUNICATIONS BETWEEN DEVICES CONNECTED RESPECTIVELY TO PUBLIC NETWORKS SUCH AS THE INTERNET AND TO PRIVATE NETWORKS BY FACILITATING RESOLUTION OF HUMAN-READABLE ADDRESSES, US PAT 6557037Assignee: Sun Microsystems, (U.S. PTO Utility 2003)

C 146 SYSTEM AND METHOD FOR GENERATING DOMAIN NAMES AND FOR FACILITATING REGISTRATION AND TRANSFER OF THE SAME, US PAT 6298341Assignee: Raredomains.com, LLC, (U.S. PTO Utility 2001)

C 147 SYSTEM AND METHOD FOR HIGHLY SECURE DATA COMMUNICATIONS, US PAT APP 20020004898 (U.S. PTO Application 2002)

C 148 SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS, US PAT 7072964Assignee: Science Applications International, (U.S. PTO Utility 2006)

C 149 SYSTEM AND METHOD FOR IP NETWORK ADDRESS TRANSLATION USING SELECTIVE MASQUERADE, US PAT 6717949Assignee: International Business Machines, (U.S. PTO Utility 2004)

C 150 SYSTEM AND METHOD FOR MANAGING NETWORKS ADDRESSED VIA COMMON NETWORK ADDRESSES, US PAT 6175867Assignee: MCI World Com, Inc., (U.S. PTO Utility 2001)

C 151 SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS, US PAT 6330562Assignee: International Business Machines, (U.S. PTO Utility 2001)

C 152 SYSTEM AND METHOD FOR REDUCING LATENCIES WHILE TRANSLATING INTERNET HOST NAME- ADDRESS BINDINGS, US PAT 6262987 (U.S. PTO Utility 2001)

C 153 SYSTEM AND METHOD FOR RESOLVING FIBRE CHANNEL DEVICE ADDRESSES ON A NETWORK USING THE DEVICE&apos;S FULLY QUALIFIED DOMAIN NAME, US PAT 6199112Assignee: Crossroads Systems, Inc., (U.S. PTO Utility 2001)

C 154 SYSTEM AND METHOD OF USER AUTHENTICATION FOR NETWORK COMMUNICATION THROUGH A POLICY AGENT, US PAT 7039713Assignee: Microsoft Corporation, (U.S. PTO Utility 2006)

C 155 SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS, US PAT 6496867Assignee: 3Com Corporation, (U.S. PTO Utility 2002)

C 156 SYSTEM APPARATUS AND METHOD FOR HOSTING AND ASSIGNING DOMAIN NAMES ON A WIDE AREA NETWORK, US PAT 6687746Assignee: Ideaflood, Inc., (U.S. PTO Utility 2004)

C 157 SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE, US PAT 5878231Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1999)

C 158 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR MULTIPLE-ENTRY POINT VIRTUAL POINT OF SALE ARCHITECTURE, US PAT 6178409Assignee: VeriFone, Inc., (U.S. PTO Utility 2001)

C 159 SYSTEM PROVIDING FOR MULTIPLE VIRTUAL CIRCUITS BETWEEN TWO NETWORK ENTITIES, US PAT 6222842Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)

C 160 SYSTEMS AND METHODS FOR DETERMINING COLLECTING AND USING GEOGRAPHIC LOCATIONS OF INTERNET USERS, US PAT 6757740Assignee: Digital Envoy, Inc., (U.S. PTO Utility 2004)

C 161 SYSTEMS AND METHODS FOR DISTRIBUTED NETWORK PROTECTION, US PAT 7197563Assignee: Invicta Networks, Inc., (U.S. PTO Utility 2007)

C 162 SYSTEMS AND METHODS FOR SECURED DOMAIN NAME SYSTEM USE BASED ON PRE-EXISTING TRUST, US PAT APP 20060059337Assignee: Nokia Corporation, (U.S. PTO Application 2006)

C 163 TCP/IP ADDRESS PROTECTION MECHANISM IN A CLUSTERED SERVER ENVIRONMENT, US PAT 6430610Assignee: Steeleye Technology, Inc., (U.S. PTO Utility 2002)

C 164 TRAVEL ORGANIZER, US PAT 6179102 (U.S. PTO Utility 2001)

C 165 UNIFIED WEB-BASED INTERFACE-TO MULTIPLE REGISTRAR SYSTEMS, US PAT 7167904Assignee: Network Solutions, LLC, (U.S. PTO Utility 2007)

C 166 UNIVERSAL ACCESS MULTIMEDIA DATA NETWORK, US PAT 6101182Assignee: Bell Atlantic Network Services, Inc., (U.S. PTO Utility 2000)

C 167 UNIVERSAL ACCESS MULTIMEDIA DATA NETWORK, US PAT 5790548Assignee: Bell Atlantic Network Services, Inc., (U.S. PTO Utility 1998)

▷ 168 UNIVERSAL ELECTRONIC RESOURCE DENOTATION, REQUEST AND DELIVERY SYSTEM, US PAT 5764906Assignee: Netword LLC, (U.S. PTO Utility 1998)

C 169 USER-DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS, US PAT APP 20050055306Assignee: Science Applications International, (U.S. PTO Application 2005)

C 170 VIRTUAL DIAL-UP PROTOCOL FOR NETWORK COMMUNICATION, US PAT 6487598Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2002)

C 171 VIRTUAL DIAL-UP PROTOCOL FOR NETWORK COMMUNICATION, US PAT 6308213Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2001)

H 172 VIRTUAL DIAL-UP PROTOCOL FOR NETWORK COMMUNICATION, US PAT 5918019Assignee: Cisco Technology, Inc., (U.S. PTO Utility 1999)

C 173 VIRTUAL PRIVATE NETWORK SYSTEM OVER PUBLIC MOBILE DATA NETWORK AND VIRTUAL LAN, US PAT 6016318Assignee: NEC Corporation, (U.S. PTO Utility 2000)

C 174 WEB-BASED ADMINISTRATION OF IP TUNNELING ON INTERNET FIREWALLS, US PAT 5864666Assignee: International Business Machines, (U.S. PTO Utility 1999)

C 175 WORLD-WIDE-WEB SERVER WITH DELAYED RESOURCE-BINDING FOR RESOURCE-BASED LOAD BALANCING ON A DISTRIBUTED RESOURCE MULTI-NODE NETWORK, US PAT 5774660Assignee: Resonate, Inc., (U.S. PTO Utility 1998)

US District Court Civil Docket

U.S. District - Texas Eastern
(Tyler)

6:11cv563

Virnetx Inc v. Apple Inc

This case was retrieved from the court on Friday, April 06, 2012

Date Filed:	**11/01/2011**	Class Code:	**OPEN**
Assigned To:	**Judge Leonard Davis**	Closed:	**No**
Referred To:		Statute:	**35:271**
Nature of suit:	**Patent (830)**	Jury Demand:	**Plaintiff**
Cause:	**Patent Infringement**	Demand Amount:	**$0**
Lead Docket:	**None**	NOS Description:	**Patent**
Other Docket:	**None**		
Jurisdiction:	**Federal Question**		

Litigants	Attorneys
Virnetx Inc Plaintiff	Douglas A Cawley [COR LD NTC] McKool Smith -Dallas 300 Crescent Court Suite 1500 Dallas , TX 75201 USA 214/ 978-4972 Fax: 12149784044 Email: Dcawley@mckoolsmith.com
Apple Inc Defendant	Danny Lloyd Williams [COR LD NTC] Williams Morgan & Amerson 10333 Richmond Suite 1100 Houston , TX 77042 USA 713/ 934-4060 Fax: 17139347011 Email: Dwilliams@wmalaw.com

Date	#	Proceeding Text	Source
11/01/2011	1	COMPLAINT against Apple Inc. (Filing fee $ 350 receipt number 0540-3299070.), filed by VirnetX Inc.. (Attachments: # 1 Civil Cover Sheet)(Cawley, Douglas) (Entered: 11/01/2011)	
11/01/2011	2	CORPORATE DISCLOSURE STATEMENT filed by VirnetX Inc. identifying Corporate Parent VirnetX Holding Corporation for VirnetX Inc.. (Cawley, Douglas) (Entered: 11/01/2011)	
11/01/2011	3	Notice of Filing of Patent/Trademark Form (AO 120). AO 120 mailed to the Director of the U.S. Patent and Trademark Office. (Cawley, Douglas) (Entered: 11/01/2011)	
11/01/2011	--	Judge Leonard Davis added. (mll,) (Entered: 11/01/2011)	
11/01/2011	4	E-GOV SEALED SUMMONS Issued as to Apple Inc., and emailed to pltf for service. (mll,) (Entered: 11/01/2011)	
11/10/2011	5	Return of Service Executed as to Apple Inc. on 11/2/2011, by personal service; answer due:	

		11/23/2011. (mll,) (Entered: 11/10/2011)
11/18/2011	6	Defendant's Unopposed First Application for Extension of Time to Answer Complaint re Apple Inc.. (Williams, Danny) (Entered: 11/18/2011)
11/21/2011	--	Defendant's Unopposed First Application for Extension of Time to Answer Complaint 6 is granted pursuant to Local Rule CV-12 for Apple Inc. to 12/23/2011. 30 Days Granted for Deadline Extension.(mll,) (Entered: 11/21/2011)
12/07/2011	7	Unopposed MOTION to Stay OF PROCEEDINGS PURSUANT TO 28 U.S.C. &#167; 1659(a) by Apple Inc.. (Attachments: # 1 Text of Proposed Order)(Williams, Danny) (Entered: 12/07/2011)
12/07/2011	8	Additional Attachments to Main Document: 7 Unopposed MOTION to Stay OF PROCEEDINGS PURSUANT TO 28 U.S.C. &#167; 1659(a) .. (Attachments: # 1 Exhibit A)(Williams, Danny) (Entered: 12/07/2011)
12/15/2011	9	ORDER granting 7 Motion to Stay. This civil action is STAYED until the determination of the International Trade Commission in Investigation No. 337-TA-818 becomes final. Signed by Judge Leonard Davis on 12/15/11. cc:attys 12-16-11 (mll,) (Entered: 12/16/2011)

UNITED STATES PATENT AND TRADEMARK OFFICE GRANTED PATENT

8051181

Get Drawing Sheet 1 of 40
Access PDF of Official Patent *
Order Patent File History / Wrapper from REEDFAX®
Link to Claims Section

November 1, 2011

Method for establishing secure communication link between computers of virtual private network

REEXAM-LITIGATE:

NOTICE OF LITIGATION

Virnetx Inc v. Apple Inc, Filed November 1, 2011, D.C. E.D. Texas, Doc. No. 6:11cv563

INVENTOR: Larson, Victor - Fairfax, Virginia, United States of America (US), United States of America () ; Short, III, Robert Dunham - Leesburg, Virginia, United States of America (US), United States of America () ; Munger, Edmund Colby - Crownsville, Maryland, United States of America (US), United States of America () ; Williamson, Michael - South Riding, Virginia, United States of America (US), United States of America ()

CERT-CORRECTION:
January 3, 2012 - a Certificate of Correction was issued for this patent (O.G. January 24, 2012)

APPL-NO: 679416 (11)

FILED-DATE: February 27, 2007

GRANTED-DATE: November 1, 2011

ASSIGNEE-PRE-ISSUE:
June 21, 2007 - ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, 10260 CAMPUS POINT DRIVE, SAN DIEGO, CALIFORNIA, UNITED STATES OF AMERICA (US), 92121, Reel and Frame Number: 019463/0762
June 21, 2007 - ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., VIRNETX, INC., 5615 SCOTTS VALLEY DRIVE, SUITE 110, SCOTTS VALLEY, CALIFORNIA, UNITED STATES OF AMERICA (US), 95066, Reel and Frame Number: 019464/0133

ASSIGNEE-AT-ISSUE:
Virnetx, Inc., Scotts Valley, California, United States of America (US), United States company or corporation (02)

ASSIGNEE-AFTER-ISSUE:
January 19, 2012 - CHANGE OF ADDRESS OF ASSIGNEE, VIRNETX INC., P.O. BOX 439, ZEPHYR COVE, NEVADA, UNITED STATES OF AMERICA (US), 89448, Reel and Frame Number: 027558/0281

LEGAL-REP: McDermott Will & Emery LLP

PUB-TYPE: November 1, 2011 - Patent with a pre-grant publication (B2)

PUB-COUNTRY: United States of America (US)

LEGAL-STATUS:

June 21, 2007 - ASSIGNMENT
June 21, 2007 - ASSIGNMENT
June 21, 2007 - ASSIGNMENT
January 3, 2012 - CERTIFICATE OF CORRECTION
January 19, 2012 - ASSIGNMENT

FILING-LANG: English (EN) (ENG)

PUB-LANG: English (EN) (ENG)

REL-DATA:

Division of Ser. No. 09558209, April 26, 2000, ABANDONED
, which is a Continuation-in-part of Ser. No. 09504783, February 15, 2000, GRANTED 6502135
, which is a Continuation-in-part of Ser. No. 09429643, October 29, 1999, GRANTED 7010604
Provisional Application Ser. No. 60106261, October 30, 1998, PENDING
Provisional Application Ser. No. 60137704, June 7, 1999, PENDING
Prior Publication 20080005792, January 3, 2008, Patent Application Publication (A1)

US-MAIN-CL: 709#227

US-ADDL-CL: 709#228

CL: 709

SEARCH-FLD: 709#225-229, 709#245

IPC-MAIN-CL: [8] G06F 015#173 (20060101) Advanced Inventive 20111101 (A F I B H US)

IPC-ADDL-CL: [8] H04L 012#56 (20060101) Advanced Inventive 20051008 (A I R M EP)

IPC-ADDL-CL: [8] H04L 029#06 (20060101) Advanced Inventive 20051008 (A I R M EP)

IPC-ADDL-CL: [8] H04L 029#12 (20060101) Advanced Inventive 20051008 (A I R M EP)

REF-CITED:

2895502, July 21, 1959, Garland Roper Charles et al., United States of America (US)
4920484, April 24, 1990, Ranade, United States of America (US)
4933846, June 12, 1990, Humphrey et al., United States of America (US)
4988990, January 29, 1991, Warrior, United States of America (US)
5164988, November 17, 1992, Matyas, United States of America (US)
5276735, January 4, 1994, Boebert et al., United States of America (US)
5303302, April 12, 1994, Burrows, United States of America (US)
5311593, May 10, 1994, Carmi, United States of America (US)
5329521, July 12, 1994, Walsh et al., United States of America (US)
5341426, August 23, 1994, Barney et al., United States of America (US)
5367643, November 22, 1994, Chang et al., United States of America (US)
5384848, January 24, 1995, Kikuchi, United States of America (US)
5511122, April 23, 1996, Atkinson, United States of America (US)
5559883, September 24, 1996, Williams, United States of America (US)
5561669, October 1, 1996, Lenney et al., United States of America (US)
5588060, December 24, 1996, Aziz, United States of America (US)
5590285, December 31, 1996, Krause et al., United States of America (US)
5625626, April 29, 1997, Umekita, United States of America (US)
5629984, May 13, 1997, McManis, United States of America (US)
5654695, August 5, 1997, Olnowich et al., United States of America (US)
5682480, October 28, 1997, Nakagawa, United States of America (US)
5689566, November 18, 1997, Nguyen, United States of America (US)
5740375, April 14, 1998, Dunne et al., United States of America (US)
5764906, June 9, 1998, Edelstein et al., United States of America (US)

5771239, June 23, 1998, Moroney et al., United States of America (US)
5774660, June 30, 1998, Brendel et al., United States of America (US)
5787172, July 28, 1998, Arnold, United States of America (US)
5790548, August 4, 1998, Sistanizadeh et al., United States of America (US)
5796942, August 18, 1998, Esbensen, United States of America (US)
5805801, September 8, 1998, Holloway et al., United States of America (US)
5805803, September 8, 1998, Birrell et al., United States of America (US)
5822434, October 13, 1998, Caronni et al., United States of America (US)
5842040, November 24, 1998, Hughes et al., United States of America (US)
5845091, December 1, 1998, Dunne et al., United States of America (US)
5864666, January 26, 1999, Shrader, United States of America (US)
5867650, February 2, 1999, Osterman, United States of America (US)
5870610, February 9, 1999, Beyda et al., United States of America (US)
5878231, March 2, 1999, Baehr et al., United States of America (US)
5892903, April 6, 1999, Klaus, United States of America (US)
5898830, April 27, 1999, Wesinger et al., United States of America (US)
5905859, May 18, 1999, Holloway et al., United States of America (US)
5918018, June 29, 1999, Gooderum et al., United States of America (US)
5918019, June 29, 1999, Valencia, United States of America (US)
5950195, September 7, 1999, Stockwell et al., United States of America (US)
5996016, November 30, 1999, Thalheimer et al., United States of America (US)
6006259, December 21, 1999, Adelman et al., United States of America (US)
6006272, December 21, 1999, Aravamudan et al., United States of America (US)
6016318, January 18, 2000, Tomoike, United States of America (US)
6016512, January 18, 2000, Huitema, United States of America (US)
6041342, March 21, 2000, Yamaguchi, United States of America (US)
6052788, April 18, 2000, Wesinger et al., United States of America (US)
6055574, April 25, 2000, Smorodinsky et al., United States of America (US)
6061346, May 9, 2000, Nordman, United States of America (US)
6061736, May 9, 2000, Rochberger et al., United States of America (US)
6079020, June 20, 2000, Liu, United States of America (US)
6081900, June 27, 2000, Subramaniam et al., United States of America (US)
6092200, July 18, 2000, Muniyappa et al., United States of America (US)
6101182, August 8, 2000, Sistanizadeh et al., United States of America (US)
6119171, September 12, 2000, Alkhatib, United States of America (US)
6119234, September 12, 2000, Aziz et al., United States of America (US)
6147976, November 14, 2000, Shand et al., United States of America (US)
6157957, December 5, 2000, Berthaud, United States of America (US)
6158011, December 5, 2000, Chen et al., United States of America (US)
6168409, January 2, 2001, Fare, United States of America (US)
6173399, January 9, 2001, Gilbrech, United States of America (US)
6175867, January 16, 2001, Taghadoss, United States of America (US)
6178409, January 23, 2001, Weber et al., United States of America (US)
6178505, January 23, 2001, Schneider et al., United States of America (US)
6179102, January 30, 2001, Weber et al., United States of America (US)
6199112, March 6, 2001, Wilson, United States of America (US)
6202081, March 13, 2001, Naudus, United States of America (US)
6222842, April 24, 2001, Sasyan et al., United States of America (US)
6223287, April 24, 2001, Douglas et al., United States of America (US)
6226748, May 1, 2001, Bots et al., United States of America (US)
6226751, May 1, 2001, Arrow et al., United States of America (US)
6233618, May 15, 2001, Shannon, United States of America (US)
6243360, June 5, 2001, Basilico, United States of America (US)
6243749, June 5, 2001, Sitaraman et al., United States of America (US)
6243754, June 5, 2001, Guerin et al., United States of America (US)
6246670, June 12, 2001, Karlsson et al., United States of America (US)
6256671, July 3, 2001, Strentzsch et al., United States of America (US)
6262987, July 17, 2001, Mogul, United States of America (US)
6263445, July 17, 2001, Blumenau, United States of America (US)
6286047, September 4, 2001, Ramanathan et al., United States of America (US)
6298341, October 2, 2001, Mann et al., United States of America (US)

6301223, October 9, 2001, Hrastar et al., United States of America (US)
6308213, October 23, 2001, Valencia, United States of America (US)
6308274, October 23, 2001, Swift, United States of America (US)
6311207, October 30, 2001, Mighdoll et al., United States of America (US)
6314463, November 6, 2001, Abbott et al., United States of America (US)
6324161, November 27, 2001, Kirch, United States of America (US)
6330562, December 11, 2001, Boden et al., United States of America (US)
6332158, December 18, 2001, Risley et al., United States of America (US)
6333272, December 25, 2001, McMillin et al., United States of America (US)
6338082, January 8, 2002, Schneider, United States of America (US)
6353614, March 5, 2002, Borella et al., United States of America (US)
6425003, July 23, 2002, Herzog et al., United States of America (US)
6430155, August 6, 2002, Davie et al., United States of America (US)
6430610, August 6, 2002, Carter, United States of America (US)
6487598, November 26, 2002, Valencia, United States of America (US)
6502135, December 31, 2002, Munger et al., United States of America (US)
6505232, January 7, 2003, Mighdoll et al., United States of America (US)
6510154, January 21, 2003, Mayes et al., United States of America (US)
6549516, April 15, 2003, Albert et al., United States of America (US)
6557037, April 29, 2003, Provino, United States of America (US)
6571296, May 27, 2003, Dillon, United States of America (US)
6571338, May 27, 2003, Shaio et al., United States of America (US)
6581166, June 17, 2003, Hirst et al., United States of America (US)
6606708, August 12, 2003, Devine et al., United States of America (US)
6618761, September 9, 2003, Munger et al., United States of America (US)
6671702, December 30, 2003, Kruglikov et al., United States of America (US)
6687551, February 3, 2004, Steindl, United States of America (US)
6687746, February 3, 2004, Shuster et al., United States of America (US)
6701437, March 2, 2004, Hoke et al., United States of America (US)
6714970, March 30, 2004, Fiveash et al., United States of America (US)
6717949, April 6, 2004, Boden et al., United States of America (US)
6751738, June 15, 2004, Wesinger, Jr. et al., United States of America (US)
6752166, June 22, 2004, Lull et al., United States of America (US)
6757740, June 29, 2004, Parekh et al., United States of America (US)
6760766, July 6, 2004, Sahlqvist, United States of America (US)
6826616, November 30, 2004, Larson et al., United States of America (US)
6839759, January 4, 2005, Larson et al., United States of America (US)
6937597, August 30, 2005, Rosenberg et al., United States of America (US)
7010604, March 7, 2006, Munger et al., United States of America (US)
7039713, May 2, 2006, Van Gunter et al., United States of America (US)
7072964, July 4, 2006, Whittle et al., United States of America (US)
7133930, November 7, 2006, Munger et al., United States of America (US)
7167904, January 23, 2007, Devarajan et al., United States of America (US)
7188175, March 6, 2007, McKeeth, United States of America (US)
7188180, March 6, 2007, Larson et al., United States of America (US)
7197563, March 27, 2007, Sheymov et al., United States of America (US)
7353841, April 8, 2008, Kono et al., United States of America (US)
7461334, December 2, 2008, Lu et al., United States of America (US)
7490151, February 10, 2009, Munger et al., United States of America (US)
7493403, February 17, 2009, Shull et al., United States of America (US)
20010049741, December 6, 2001, Skene et al., United States of America (US)
20020004898, January 10, 2002, Droge, United States of America (US)
20030196122, October 16, 2003, Wesinger, Jr. et al., United States of America (US)
20040199493, October 7, 2004, Ruiz et al., United States of America (US)
20040199520, October 7, 2004, Ruiz et al., United States of America (US)
20040199608, October 7, 2004, Rechterman et al., United States of America (US)
20040199620, October 7, 2004, Ruiz et al., United States of America (US)
20050055306, March 10, 2005, Miller et al., United States of America (US)
20060059337, March 16, 2006, Poyhonen et al., United States of America (US)
20070208869, September 6, 2007, Adelman et al., United States of America (US)
20070214284, September 13, 2007, King et al., United States of America (US)

20070266141, November 15, 2007, Norton, United States of America (US)
20080235507, September 25, 2008, Ishikawa et al., United States of America (US)
19924575, December 2, 1999, Federal Republic of Germany (DE)
838930, April 29, 1998, European Patent Office (EP)
814589, December 29, 1997, European Patent Office (EP)
814589, December 29, 1997, European Patent Office (EP)
838930, April 29, 1998, European Patent Office (EP)
836306, April 15, 1998, European Patent Office (EP)
836306, April 15, 1998, European Patent Office (EP)
858189, August 12, 1998, European Patent Office (EP)
2317792, April 1, 1998, United Kingdom of Great Britain and Northern Ireland (GB)
2317792, April 1, 1998, United Kingdom of Great Britain and Northern Ireland (GB)
2334181, August 11, 1999, United Kingdom of Great Britain and Northern Ireland (GB)
2334181, August 11, 1999, United Kingdom of Great Britain and Northern Ireland (GB)
2340702, February 23, 2000, United Kingdom of Great Britain and Northern Ireland (GB)
62214744, September 21, 1987, Japan (JP)
04363941, December 16, 1992, Japan (JP)
09018492, January 17, 1997, Japan (JP)
10070531, March 10, 1998, Japan (JP)
98027783, June, 1998, World Intellectual Property Organization (WIPO) (WO)
98027783, June, 1998, World Intellectual Property Organization (WIPO) (WO)
98027783, June, 1998, World Intellectual Property Organization (WIPO) (WO)
98043396, October, 1998, World Intellectual Property Organization (WIPO) (WO)
98055930, December, 1998, World Intellectual Property Organization (WIPO) (WO)
98059470, December, 1998, World Intellectual Property Organization (WIPO) (WO)
99011019, March, 1999, World Intellectual Property Organization (WIPO) (WO)
99038081, July, 1999, World Intellectual Property Organization (WIPO) (WO)
99048303, September, 1999, World Intellectual Property Organization (WIPO) (WO)
00017775, March, 2000, World Intellectual Property Organization (WIPO) (WO)
01017775, March, 2000, World Intellectual Property Organization (WIPO) (WO)
00070458, November, 2000, World Intellectual Property Organization (WIPO) (WO)
01016766, March, 2001, World Intellectual Property Organization (WIPO) (WO)
01050688, July, 2001, World Intellectual Property Organization (WIPO) (WO)

NON-PATENT LITERATURE:

Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.

Microsoft Corporation's Fifth Amended Invalidity Contentions dated Sep. 18, 2009, *VirnetX Inc. and Science Applications International Corp.* v. , *Microsoft Corporation* and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759.*VirnetX Inc. and Science Applications International Corp. Microsoft Corporation*

The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol;" Network Working Group, RFC 2401 (Nov. 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (Nov. 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html.(–)

Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (Nov. 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (Jul. 1996) ("Galvin").

WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000).*WatchGuard Firebox System Powerpoint*

WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999).*MSS Firewall Specifications*

WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000).*Request for Information, Security Services*

WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (Feb. 2000).*Protecting the Internet Distributed Enterprise, White Paper*

WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14, 2000) (resubmitted).*WatchGuard LiveSecurity for MSS Powerpoint*

WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes* (Jul. 21, 2000).*MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes*

DNS-related correspondence dated Sep. 7, 1993 to Sep. 20, 1993. (Pre KX, KX Records).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 2, 1996). (RFC 2543 Internet Draft 1).

Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail).

Aventail Corp., "Socks Version 5," Aventail Whitepaper, available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Mar. 27, 1997). (RFC 2543 Internet Draft 2).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 31, 1997). (RFC 2543 Internet Draft 3).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 11, 1997). (RFC 2543 Internet Draft 4).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (May 14, 1998). (RFC 2543 Internet Draft 5).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jun. 17, 1998). (RFC 2543 Internet Draft 6).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 16, 1998). (RFC 2543 Internet Draft 7).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Aug. 7, 1998). (RFC 2543 Internet Draft 8).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Sep. 18, 1998). (RFC 2543 Internet Draft 9).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 12, 1998). (RFC 2543 Internet Draft 10).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 15, 1998). (RFC 2543 Internet Draft 11).

Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail).

Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail).

Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail).

Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jan. 15, 1999). (RFC 2543 Internet Draft 12).

Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW).*Check Point FireWall-1 Administration Guide*

Assured Digital Products. (Assured Digital).

F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3).*F-Secure Evaluation Kit*

F-Secure, *F-Secure Evaluation Kit* (Sep. 1998) (FSECURE 00000009) (Evaluation Kit 9).*F-Secure Evaluation Kit*

IRE, Inc., *SafeNet/Soft-PK Version 4* (Mar. 28, 2000) (Soft-PK Version 4).*SafeNet/Soft-PK Version 4*

IRE/SafeNet Inc., *VPN Technologies Overview* (Mar. 28, 2000) (Safenet VPN Overview).*VPN Technologies Overview*

IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager).*SafeNet/VPN Policy Manager Quick Start Guide Version 1*

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000).*Dynamic Virtual Private Networks Presentation v.3*

David Kosiur, "Building and Managing Virtual Private Networks" (1998).

P. Mockapetris, "Domain Names—Implementation and Specification," Network Working Group, RFC 1035 (Nov. 1987).

Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.

Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.

Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998).

D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, Dec. 5, 1958, First Edition, first copy, p. 102-108.

Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998).

Chapman et al., "Domain Name System (DNS)," 278-296 (1995).

Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), vol. 1729; 85-102 (1999).

De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999).

Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998).

Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pp. 122-131 (1999).

Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000).

Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pp. 399-440 (1999).

Takata, "U.S. Vendors Take Serious Action to Act Against Crackers—A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87 (1997).

Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998).

PCT International Search Report for related PCT Application No. PCT/US01/13261, 8 pages.

PCT International Search Report for related PCT Application No. PCT/US99/25323, 3 pages.

PCT International Search Report for related PCT Application No. PCT/US99/25325, 3 pages.

Non-Final Office Action dated Jun. 16, 2003 from corresponding U.S. Appl. No. 09/429,643.

Final Office Action dated Feb. 11, 2004 from corresponding U.S. Appl. No. 09/429,643.

Notice of Allowance dated May 27, 2009 from corresponding U.S. Appl. No. 11/839,969.

Non-Final Office Action dated Mar. 1, 2004 from corresponding U.S. Appl. No. 10/401,888.

Non-Final Office Action dated May 4, 2004 from corresponding U.S. Appl. No. 09/429,643.

Non-Final Office Action dated Jun. 24, 2004 from corresponding U.S. Appl. No. 10/259,494.

Notice of Allowance dated Jul. 21, 2004 from corresponding U.S. Appl. No. 10/401,888.

Notice of Allowance dated Aug. 16, 2004 from corresponding U.S. Appl. No. 10/702,580.
Notice of Allowance dated Aug. 17, 2004 from corresponding U.S. Appl. No. 10/702,522.
Non-Final Office Action dated Oct. 21, 2004 from corresponding U.S. Appl. No. 10/401,551.
Final Office Action dated Apr. 11, 2005 from corresponding U.S. Appl. No. 09/429,643.
Non-Final Office Action dated Jun. 3, 2005 from corresponding U.S. Appl. No. 10/401,551.
Notice of Allowance dated Aug. 10, 2005 from corresponding U.S. Appl. No. 09/429,643.
Non-Final Office Action dated Oct. 18, 2005 from corresponding U.S. Appl. No. 10/259,494.
Notice of Allowance dated Dec. 5, 2005 from corresponding U.S. Appl. No. 09/429,643.
Final Office Action dated Dec. 7, 2005 from corresponding U.S. Appl. No. 10/401,551.
Notice of Allowance dated Feb. 16, 2006 from corresponding U.S. Appl. No. 10/401,551.
Notice of Allowance dated Mar. 17, 2006 from corresponding U.S. Appl. No. 10/401,551.
Non-Final Office Action dated Mar. 28, 2006 from corresponding U.S. Appl. No. 10/259,494.
Notice of Allowance dated Apr. 5, 2006 from corresponding U.S. Appl. No. 10/401,551.
Notice of Allowance dated Apr. 18, 2006 from corresponding U.S. Appl. No. 10/401,551.
Notice of Allowance dated May 9, 2006 from corresponding U.S. Appl. No. 10/401,551.
Non-Final Office Action dated May 19, 2006 from corresponding U.S. Appl. No. 10/702,486.
Non-Final Office Action dated Oct. 30, 2006 from corresponding U.S. Appl. No. 10/259,494.
Notice of Allowance dated Nov. 21, 2006 from corresponding U.S. Appl. No. 10/702,486.
Non-Final Office Action dated Mar. 21, 2007 from corresponding U.S. Appl. No. 10/714,849.
Non-Final Office Action dated Jun. 15, 2007 from corresponding U.S. Appl. No. 10/259,494.
Notice of Allowance dated Oct. 29, 2007 from corresponding U.S. Appl. No. 10/714,849.
Notice of Allowance dated Jan. 11, 2008 from corresponding U.S. Appl. No. 10/259,494.
Notice of Allowance dated Apr. 10, 2008 from corresponding U.S. Appl. No. 10/714,849.
Notice of Allowance dated Jul. 1, 2008 from corresponding U.S. Appl. No. 10/259,494.
Non-Final Office Action dated Sep. 17, 2008 from corresponding U.S. Appl. No. 11/839,969.
Deposition Transcript for Gary Tomlinson dated Feb. 27, 2009.
Non-Final Office Action dated Mar. 5, 2009 from corresponding U.S. Appl. No. 11/301,022.
Notice of Allowance dated Apr. 3, 2009 from corresponding U.S. Appl. No. 11/839,969.
Non-Final Office Action dated Jun. 9, 2009 from corresponding U.S. Appl. No. 11/839,987.
Non-Final Office Action dated Sep. 2, 2009 from corresponding U.S. Appl. No. 11/924,460.
Notice of Allowance dated Sep. 16, 2009 from corresponding U.S. Appl. No. 11/839,969.
Notice of Allowance dated Nov. 19, 2009 from corresponding U.S. Appl. No. 11/839,969.
Final Office Action dated Jan. 6, 2010 from corresponding U.S. Appl. No. 11/839,987.
Notice of Allowance dated Jan. 13, 2010 from corresponding U.S. Appl. No. 11/839,969.
Notice of Allowance dated Jan. 28, 2010 from corresponding U.S. Appl. No. 11/840,508.
Final Office Action dated Feb. 9, 2010 from corresponding U.S. Appl. No. 11/301,022.
Notice of Allowance dated Feb. 24, 2010 from corresponding U.S. Appl. No. 11/839,987.
Non-Final Office Action dated Mar. 19, 2010 from corresponding U.S. Appl. No. 11/840,560.
Non-Final Office Action dated Jun. 7, 2010 from corresponding U.S. Appl. No. 11/924,460.
Non-Final Office Action dated Jun. 9, 2010 from corresponding U.S. Appl. No. 11/924,460.
Non-Final Office Action dated Jul. 1, 2010 from corresponding U.S. Appl. No. 11/839,969.
Non-Final Office Action dated Jul. 8, 2010 from corresponding U.S. Appl. No. 11/839,987.
Non-Final Office Action dated Jul. 14, 2010 from corresponding U.S. Appl. No. 11/840,508.
Final Office Action dated Oct. 21, 2010 from corresponding U.S. Appl. No. 11/840,560.
Non-Final Office Action dated Dec. 14, 2010 from corresponding U.S. Appl. No. 11/839,937.
Notice of Allowance dated Jan. 4, 2011 from corresponding U.S. Appl. No. 11/301,022.
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 10, 2010, 9:00 AM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 10, 2010, 1:00 PM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 11, 2010, 9:00 AM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 11, 2010, 1:30 PM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 12, 2010, 9:00 AM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 12, 2010, 1:15 PM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 15, 2010, 9:00 AM.*VirnetX Microsoft Corporation*
Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 15, 2010, 12:35 PM.*VirnetX Microsoft*

Corporation

Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 8, 2010, 8:45 AM.*VirnetX Microsoft Corporation*

Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 8, 2010, 1:30 PM.*VirnetX Microsoft Corporation*

Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 9, 2010, 9:00 AM.*VirnetX Microsoft Corporation*

Trial Transcript, *VirnetX* vs. , *Microsoft Corporation* dated Mar. 9, 2010, 1:30 PM.*VirnetX Microsoft Corporation*

European Search Report dated Jan. 24, 2011 from corresponding European Application No. 10011949.4.

European Search Report dated Mar. 17, 2011 from corresponding European Application No. 10184502.2.

Hollenbeck et al., Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999).

Notice of Allowance dated Mar. 14, 2011 from corresponding U.S. Appl. No. 11/840,508.

Tannenbaum, "Computer Networks," pp. 202-219 (1996).

Defendants' Preliminary Joint Invalidity Contentions dated Jul. 1, 2011.

Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated Jul. 1, 2011.

Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated Jul. 1, 2011.

Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 3, RFC 2543[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 4, RFC 2543[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 5, RFC 2543[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 6, SIP Draft v.2[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 7, SIP Draft v.2[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 8, SIP Draft v.2[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 9, H.323[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 10, H.323[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 11, H.323[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 12, SSL 3.0[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 13, SSL 3.0[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 14, SSL 3.0[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 15, RFC 2487[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 16, RFC 2487[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 17, RFC 2487[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 18, RFC 2595[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 19, RFC 2595[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 20, RFC 2595[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 21, iPass[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 22, iPASS[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 23, iPASS[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 24, "US &prime;034"[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 25, US Patent No. 6,453,034 ("US &prime;034")[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 26, US Patent No. 6,453,034 ("US &prime;034")[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 27, US &prime;287[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 28, US &prime;287[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 29, US &prime;287[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 30, Overview of Access VPNs[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)

Exhibit 31, Overview of Access VPNs[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 32, Overview of Access VPNs[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)

Exhibit 34, RFC 1928[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 35, RFC 1928[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 36, RFC 1928[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 37, RFC 2661[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 38, RFC 2661[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 39, RFC 2661[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 40, SecureConnect[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 41, SecureConnect[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 42,SecureConnect[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 43, SFS-HTTP[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 44, SFS-HTTP[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 45, SFS-HTTP[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 46, US &prime;883[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 47, US &prime;883[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 48, US &prime;883[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 49, US &prime;132[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 50, US &prime;132[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 51, US &prime;132[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 52, US &prime;213[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 53, US &prime;213[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 54, US &prime;213[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 55, B&M VPNs[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 56, B&M VPNs[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 57, B&M VPNs[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 58, BorderManager[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 59, BorderManager[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 60, BorderManager[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 61, Prestige 128 Plus[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 62, Prestige 128 Plus[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 63, Prestige 128 Plus[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 64, RFC 2401[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 65, RFC 2401[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 66, RFC 2401[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 67, RFC 2486[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 68, RFC 2486[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 69, RFC 2486[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 70, Understanding IPSec[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 71, Understanding IPSec[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 72, Understanding IPSec[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 73, US &prime;820[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 74, US &prime;820[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 75, US &prime;820[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 76, US &prime;019[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 77, US &prime;019[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 78, US &prime;049[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 79, US &prime;049[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 80, US &prime;049[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 81, US &prime;748[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 82, US &prime;261[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 83, US &prime;261[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)

Exhibit 84, US &prime;261[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 85, US &prime;900[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 86, US &prime;900[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 87, US &prime;900[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 88, US &prime;671[1] vs, Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 89, US &prime;671[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 90, US &prime;671[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 91, JP &prime;704[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 92, JP &prime;704[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 93, JP &prime;704[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 94, GB &prime;841[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 95, GB &prime;841[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 96, GB &prime;841[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 97, US &prime;318[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 98, US &prime;318[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 99, US &prime;318[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 100, VPN/VLAN[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 101, Nikkei[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 102, Nikkei[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 103, Nikkei[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 104, Special Anthology[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 105, Omron[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 106, Gauntlet System[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 107, Gauntlet System[1] vs. Claims of the &prime;151 Patent′ [2].(1)(2)
Exhibit 108, Gauntlet System[1] vs. Claims of the &prime;180 Patent′ [2].(1)(2)
Exhibit 109, Gauntlet System[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 110, Gauntlet System[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 111, Gauntlet System[1] vs. Claims of the &prime;759 Patent′ [2].(1)(2).
Exhibit 112, IntraPort System[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 113, IntraPort System[1] vs. Claims of the &prime;151 Patent′ [2].(1)(2)
Exhibit 114, IntraPort System[1] vs. Claims of the &prime;180 Patent′ [2].(1)(2)
Exhibit 115, IntraPort System[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 116, IntraPort System[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 117, IntraPort System[1] vs. Claims of the &prime;759 Patent′ [2].(1)(2)
Exhibit 118, Altiga VPN System[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 119, Altiga VPN System[1] vs. Claims of the &prime;151 Patent′ [2].(1)(2)
Exhibit 120, Altiga VPN System[1] vs. Claims of the &prime;180 Patent′ [2].(1)(2)
Exhibit 121, Altiga VPN System[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 122, Altiga VPN System[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 123, Altiga VPN System[1] vs. Claims of the &prime;759 Patent′ [2].(1)(2)
Exhibit 124, Kiuchi[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 125, Kiuchi[1] vs. Claims of the &prime;151 Patent′ [2].(1)(2)
Exhibit 126, Kiuchi[1] vs. Claims of the &prime;180 Patent′ [2].(1)(2)
Exhibit 127, Kiuchi[1] vs. Claims of the &prime;211 Patent′ [2].(1)(2)
Exhibit 128, Kiuchi[1] vs. Claims of the &prime;504 Patent′ [2].(1)(2)
Exhibit 129, Kiuchi[1] vs. Claims of the &prime;759 Patent′ [2].(1)(2)
Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the &prime;135 Patent′ [2].(1)(2)
Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the &prime;151 Patent′ [2].(1)(2)

Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)
Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 135, Overview[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 136, RFC 2401[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 137, Schulzrinne[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 138, Schulzrinne[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 139, Schulzrinne[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 140, Schulzrinne[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)
Exhibit 141, Schulzrinne[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 142, Schulzrinne[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 143, Solana[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 144, Solana[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 145, Solana[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 146, Solana[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)
Exhibit 147, Solana[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 148, Solana[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 149, Atkinson[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 150, Atkinson[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 151, Atkinson[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 152, Atkinson[1] vs. Claims of the '211 Patent' [2].(1)(2)
Exhibit 153, Atkinson[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 154, Atkinson[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 155, Marino[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 156, Marino[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 157, Marino[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 158, Marino[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)
Exhibit 159, Marino[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 160, Marino[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 161, Aziz (&prime;646)[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 162, VVesinger[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 163, Wesinger[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 164, Wesinger[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 165, Wesinger[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)
Exhibit 166, Wesinger[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 167, Wesinger[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 168, Aziz (&prime;234)[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 169, Aziz (&prime;234)[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 170, Aziz (&prime;234)[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 171, Aziz (&prime;234)[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)
Exhibit 172, Aziz (&prime;234)[1] vs. Claims of the &prime;504 Patent' [2].(1)(2)
Exhibit 173, Aziz (&prime;234)[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 174, Schneider[1] vs. Claims of the &prime;759 Patent' [2].(1)(2)
Exhibit 175, Valencia[1] vs. Claims of the &prime;135 Patent' [2].(1)(2)
Exhibit 176, Valencia[1] vs. Claims of the &prime;151 Patent' [2].(1)(2)
Exhibit 177, Valencia[1] vs. Claims of the &prime;180 Patent' [2].(1)(2)
Exhibit 178, Valencia[1] vs. Claims of the &prime;211 Patent' [2].(1)(2)

Exhibit 179, Valencia[1] vs. Claims of the &prime;504 Patent′ 2.(1)(2)
Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867[1] vs. Claims of the &prime;180 Patent ′ 2.(1)(2)
Exhibit 181, Davison[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 182, Davison[1] vs. Claims of the &prime;151 Patent′ 2.(1)(2)
Exhibit 183, Davison[1] vs. Claims of the &prime;180 Patent′ 2.(1)(2)
Exhibit 184, Davison[1] vs. Claims of the &prime;211 Patent′ 2.(1)(2)
Exhibit 185, Davison[1] vs. Claims of the &prime;504 Patent′ 2.(1)(2)
Exhibit 186, Davison[1] vs. Claims of the &prime;759 Patent′ 2.(1)(2)
Exhibit 187, AutoSOCKS v2.1[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 188, AutoSOCKS v2.1[1] vs. Claims of the &prime;151 Patent′ 2.(1)(2)
Exhibit 189, AutoSOCKS v2.1 Administrator's Guide[1] vs. Claims of the &prime;180 Patent′ 2.(1)(2)
Exhibit 190, AutoSOCKS[1] vs. Claims of the &prime;759 Patent′ 2.(1)(2)
Exhibit 191, Aventail Connect 3.01/2.51[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 192, Aventail Connect v3.01/2.51[1] vs. Claims of the &prime;151 Patent′ 2.(1)(2)
Exhibit 193, Aventail Connect 3.01/2.51[1] vs. Claims of the &prime;180 Patent′ 2.(1)(2)
Exhibit 194, Aventail Connect 3.01/2.51[1] vs. Claims of the &prime;759 Patent′ 2.(1)(2)
Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the &prime;151 Patent′ 2.(1)(2)
Exhibit 197, Aventail Connect 3.1/2.6[1] vs. Claims of the &prime;180 Patent′ 2.(1)(2)
Exhibit 198, Aventail Connect 3.1/2.6[1] vs. Claims of the &prime;759 Patent′ 2.(1)(2)
Exhibit 199, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the &prime;151 Patent′ 2.(1)(2)
Exhibit 200, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 201, BinGO! vs. Claims of the &prime;180 Patent2.(2)
Exhibit 202, BinGO! vs. Claims of the &prime;759 Patent2.(2)
Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0)[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 204, Domain Name System (DNS) Security[1] vs. Claims of the &prime;211 Patent′ 2.(1)(2)
Exhibit 205, Domain Name System (DNS) Security[1] vs. Claims of the &prime;504 Patent′ 2.(1)(2)
Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the &prime;211 Patent′ 2.(1)(2)
Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the &prime;504 Patent′ 2.(1)(2)
Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the &prime;211 Patent′ 2.(1)(2)
Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the &prime;504 Patent′ 2.(1)(2)
Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the &prime;504 Patent′ 2.(1)(2)
Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published Jan. 1997[1] vs. Claims of the &prime;211 Patent′ 2.(1)(2)
Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the &prime;135 Patent′ 2.(1)(2)
Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1]

vs. Claims of the &prime;151 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 215, U.S. Patent No. 6,643,701^{1} vs. Claims of the &prime;135 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 216, U.S. Patent No. 6,643,701^{1} vs. Claims of the &prime;151 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401^{1} vs. Claims of the &prime;151 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401^{1} vs. Claims of the &prime;135 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 219, U.S. Patent No. 6,496,867^{1} vs. Claims of the &prime;211 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 220, U.S. Patent No. 6,496,867^{1} vs. Claims of the &prime;504 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"^{1} vs. Claims of the &prime;151 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 222, U.S. Patent No. 6,557,037^{1} vs. Claims of the &prime;211 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 223, U.S. Patent No. 6,557,037^{1} vs. Claims of the &prime;504 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS^{1} vs. Claims of the &prime;135 Patent′ ^{2}.$^{(1)(2)}$
Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS^{1} vs. Claims of the &prime;151 Patent′ ^{2}.$^{(1)(2)}$
Exhibit Cisco-1, Cisco's Prior Art Systems^{1} vs. Claims of the &prime;135 Patent.$^{(1)}$
Exhibit Cisco-2, Cisco's Prior Art Systems^{1} vs. Claims of the &prime;151 Patent.$^{(1)}$
Exhibit Cisco-3, Cisco's Prior Art Systems^{1} vs. Claims of the &prime;180 Patent.$^{(1)}$
Exhibit Cisco-4, Cisco's Prior Art Systems^{1} vs. Claims of the &prime;211 Patent.$^{(1)}$
Exhibit Cisco-5, Cisco's Prior Art Systems^{1} vs. Claims of the &prime;504 Patent.$^{(1)}$
Exhibit Cisco-6, Cisco's Prior Art Systems^{1} vs. Claims of the &prime;759 Patent.$^{(1)}$
Exhibit Cisco-7, Cisco's Prior Art PIX System^{1} vs. Claims of the &prime;759 Patent.$^{(1)}$
Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.
August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.
D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.
D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.
Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-66695-B, retrieved from the Internet: URL: http://www. springerlink.com/content/4uac0tb0hecoma89/fulltext.pdf> (Abstract).
Dolev, Shlomi and Ostrovsky, Rafil, Efficient Anonymous Multicast and Reception (Extended Abstract), 16 pages.
Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", Internet Draft, Apr. 1998, pp. 1-51.$^{(rd)}$
F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.
Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.
Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_ trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.$_{(—)}$
J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.

(—)
James E. Bellaire, "New Statement of Rules—Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.
Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.
Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.

Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.$_{(-)}$

P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.$_{(-)}$

Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.

RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP).

RFC 2543-SIP (dated Mar. 1999): Session Initiation Protocol (SIP or SIPS).

Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.

Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.

Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.

Search Report, IPER (dataed Nov. 13, 2002), International Applicatoin No. PCT/US01/04340.

Search Report, IPER (dated Feb. 6, 2002), International Application No. PCT/US01/13261.

Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.

Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NỲ 1986.

Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.

W. Stallings, "Cryptography and Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.

U.S. Appl. No. 60/134,547, filed May 17, 1999, Victor Sheymov.

U.S. Appl. No. 60/151,563, filed Aug. 31, 1999, Bryan Whittles.

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, *VirnetX Inc. and Science Applications International Corp.* v. , *Microsoft Corporation.VirnetX Inc. and Science Applications International Corp. Microsoft Corporation*

Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.

Concordance Table for the References Cited in Tables on pp. 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.

1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (Apr. 1989) (RFC1101, DNS SRV).

DNS-related correspondence dated Sep. 7, 1993 to Sep. 20, 1993. (Pre KX, KX Records).

R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (Aug. 5, 1993). (Atkinson NRL, KX Records).

Henning Schulzrinne, *Personal Mobility for Multimedia Services in the Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96).*Personal Mobility for Multimedia Services in the Internet*

Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology).*Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet*

"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (Mar. 1996). (Safe Surfing, Website Art).

Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing).

"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (Jun. 1996). (IPSec Minutes, FreeS/WAN).

J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, Jul. 1996. (Galvin, DNSSEC).

J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (Aug. 1996). (Gilmore DNS, FreeS/WAN).

H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (Aug. 1996-Sep. 1996). (Orman DNS, FreeS/WAN).

Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services* (, *DNS SRV*), IETF RFC 2052 (Oct. 1996). (RFC 2052, DNS SRV).*A DNS RR for specifying the location of services DNS SRV*

Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (Nov. 18, 1996).

(SSL, Underlying Security Technology).
M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 2, 1996). (RFC 2543 Internet Draft 1).
M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing).
Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista.*The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*
Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX).
Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX).
Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail).*available at*
Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail).*available at*
Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail).*available at*
Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail).*available at*
Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* htto://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail).*available at*
Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail).
Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing).*Privacy on the Internet*
Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology).*Installing Configuring and Using PPTP with Microsoft Clients and Servers*
Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology).*IP Security for Microsoft Windows NT Server 5.0*

Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology).*Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services*
Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology).*Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead*
Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology).*Understanding Point-to-Point Tunneling Protocol PPTP*
J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista).*Protecting a Private Network: The AltaVista Firewall*
Naganand Doraswamy *Implementation of Virtual Private Networks (, VPNs) , with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (Mar. 12, 1997). (Doraswamy).*Implementation of Virtual Private Networks VPNswith IPSecurity*
M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Mar. 27, 1997). (RFC 2543 Internet Draft 2).
Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication for Internet and Intranet Communication," Press Release, Apr. 3, 1997. (Secure Authentication, Aventail).
D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (Apr. 15, 1997). (Analysis, Underlying Security Technologies).
Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX).
Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition

for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX).

Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," Jun. 2, 1997. (First VPN, Aventail).

Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (Jun. 2, 1997). (Syverson, Onion Routing).

Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (Jun. 16, 1997). (AIAG Requirements, ANX).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 31, 1997). (RFC 2543 Internet Draft 3).

R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (Nov. 1997). (RFC 2230, KX Records).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 11, 1997). (RFC 2543 Internet Draft 4).

1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology).

Microsoft Corp., *Virtual Private Networking an Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology).*Virtual Private Networking an Overview*

Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology).*Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0*

"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV).*available at*

Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, Jan. 19, 1998. (VPN V2.6, Aventail).

R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, Feb. 6, 1998. (Moskowitz).

H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, vol. 2 (Mar. 29-Apr. 2, 1998). (Gateway, Schulzrinne).

C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP).

DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (May 14, 1998). (RFC 2543 Internet Draft 5).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jun. 17, 1998). (RFC 2543 Internet Draft 6).

D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (Jul. 1998). (RFC 2367).(—)

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jul. 16, 1998). (RFC 2543 Internet Draft 7).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Aug. 7, 1998). (RFC 2543 Internet Draft 8).

Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (Aug. 18, 1998). (Focus, Microsoft Prior Art VPN Technology).*Company Focuses on Quality and Customer Feedback*

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Sep. 18, 1998). (RFC 2543 Internet Draft 9).

Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (Nov. 1998). (RFC 2401, Underlying Security Technologies).

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Nov. 12, 1998). (RFC 2543 Internet Draft 10) 9.

Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (Dec. 1998). (DNSSEC-7).*Domain Name System Security Extensions*

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Dec. 15, 1998). (RFC 2543 Internet Draft 11).

Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail).

Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail).

Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail).

Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN References).

Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, Underlying Security Technologies).

Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW).

Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services* (, *DNS SRV*), <draft-ieft-dnsind-frc2052bis-02.txt> (Jan. 1999). (Gulbrandsen 99, DNS SRV).*A DNS RR for specifying the location of services DNS SRV*

C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs).*Virtual Private Networks*

M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (Jan. 15, 1999). (RFC 2543 Internet Draft 12).

Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (Jan. 28, 1999). (Goldschlag III, Onion Routing).

H. Schulzrinne, "Internet Telephony: architecture and protocols—an IETF perspective," Computer Networks, vol. 31, No. 3 (Feb. 1999). (Telephony, Schulzrinne).

M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (Dec. 1996-Mar. 1999). (Handley, RFC 2543).

FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (Mar. 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN).*Linux FreeS/WAN Compatibility Guide*

Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX).

Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (Jun. 21, 1999). (Hornstein, DNS SRV).*Distributing Kerberos KDC and Realm Information with DNS*

Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (Oct. 1999). (Bhattcharya LDAP VPN).

B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (Oct. 15, 1999). (Patel).

Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW).*Check Point FireWall-1 Administration Guide*

"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan. 2000). (FirstVPN Microsoft).

Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services* (, *DNS SRV*), IETF RFC 2782 (Feb. 2000). (RFC 2782, DNS SRV).*A DNS RR for specifying the location of services DNS SRV*

MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (Feb. 2000). (MITRE, SIPRNET).

H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, vol. 4, No. 3. pp. 47-57 (Jul. 2000). (Application, SIP).

Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (Jun. 2001). (DARPA, VPN Systems).

ANX 101: Basic ANX Service Outline. (Outline, ANX).

ANX 201: Advanced ANX Service. (Advanced, ANX).

Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX).

Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail).

Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET).

Data Fellows F-Secure VPN+ (F-Secure VPN+).

Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET).

Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing).*Onion Routing*

Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET).

SPARTA "Dynamic Virtual Private Network." (Sparta, VPN Systems).

Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET).

Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN).

Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec).

Network Associates *Gauntlet Firewall for Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide—Unix, Firewall Products).*Gauntlet Firewall for Unix User's Guide Version 5.0*

Network Associates *Gauntlet Firewall for Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide—NT, Firewall Products).*Gauntlet Firewall for Windows NT Getting Started Guide Version 5.0*

Network Associates *Gauntlet Firewall for Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products).*Gauntlet Firewall for Unix Getting Started Guide Version 5.0*

Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (Mar. 19, 1999) (Gauntlet Unix Release Notes, Firewall Products).*Release Notes Gauntlet Firewall for Unix 5.0*

Network Associates *Gauntlet Firewall for Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products).*Gauntlet Firewall for Windows NT Administrator's Guide Version 5.0*

Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products).*Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1*

Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN).*Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0*

Network Associates *Gauntlet Firewall for UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN).*Gauntlet Firewall for UNIX Global Virtual Private Network User's Guide Version 5.0*

Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN).*Dynamic Virtual Private Networks*

Darrell Kindred *Dynamic Virtual Private Networks (, DVPN)* (Dec. 21, 1999) (Kindred DVPN, DVPN).*Dynamic Virtual Private Networks DVPN*

Dan Sterne et.al. *TIS Dynamic Security Perimeter Research Project Demonstration* (Mar. 9, 1998) (Dynamic Security Perimeter, DVPN).*TIS Dynamic Security Perimeter Research Project Demonstration*

Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (Jan. 5, 2000) (Kindred DVPN Capability, DVPN) 11.*Dynamic Virtual Private Networks Capability Description*

Oct. 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN).

James Just & Dan Sterne *Security Quickstart Task Update* (Feb. 5, 1997) (Security Quickstart, DVPN).*Security Quickstart Task Update*

Virtual Private Network Demonstration dated Mar. 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN).

GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (, IFD) , 1.1 Plan* (Mar. 10, 1998) (IFD 1.1, DVPN).*DARPA Information Assurance Program Integrated Feasibility Demonstration IFD1.1 Plan*

Microsoft Corp. Windows NT Server Product Documentation: Administration Guide—Connection Point Services, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.ms px (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)

Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide—Connection Manager, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

Microsoft Corp. Autodial Heuristics, available at http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) available at http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I).

Marc Levy, COM Internet Services (Apr. 23, 1999), available at http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy).

Markus Horstmann and Mary Kirtland, DCOM Architecture (Jul. 23, 1997), available at http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann).

Microsoft Corp., DCOM: A Business Overview (Apr. 1997), available at http://msdn2.microsoft.com/en-

us/library/ms809320(printer).aspx (DCOM Business Overview I).
Microsoft Corp., DCOM Technical Overview (Nov. 1996), available at http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I).
Microsoft Corp., DCOM Architecture White Paper (1998) available in PDC DVD-ROM (DCOM Architecture).
Microsoft Corp, DCOM—The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) available in PDC DVD-ROM (DCOM Business Overview II).
Microsoft Corp., DCOM—Cariplo Home Banking Over the Internet White Paper (Microsoft 1996) available in PDC DVD-ROM (Cariplo II).
Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) available in PDC DVD-ROM (DCOM Solutions in Action).
Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) available 12 in PDC DVD-ROM (DCOM Technical Overview II).
125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) available at http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy).
126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet).*Essential WinInet*
Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) available at http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP).
Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.ms px (Internet Connection Services I).
Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, available athttp://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II).
Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide—Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development).*available at*
Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., Jan. 15, 1999)(Mastering Windows NT Server).*Mastering Windows NT Server 4*
Hands on, Self-Paced Training for Supporting Version 4.0 371-473 (Microsoft Press 1998) (Hands on).*Hands on, Self-Paced Training for Supporting Version 4.0*
Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx. (MS PPTP).*available at*
Kenneth Gregg, et al., *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg).*Microsoft Windows NT Server Administrator's Bible*
Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access).*available at*
Microsoft Corp., Understanding PPTP (Windows NT 4.0), available at http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.).
Microsoft Corp., Windows NT 4.0: Virtual Private Networking, available at http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)
Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing).*NT Network Plumbing: Routers, Proxies, and Web Services*
Microsoft Corp., Chapter 1—Introduction to Windows NT Routing with Routing and Remote Access Service, Available at http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13.
Microsoft Corp., Windows NT Server Product Documentation: Chapter 5—Planning for Large-Scale Configurations, available at http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of

Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)

F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3).*F-Secure Evaluation Kit*

F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3).*F-Secure NameSurfer*

F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3).*F-Secure VPN Administrator's Guide*

F-Secure, *F-Secure SSH User's & , Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3).*F-Secure SSH User's Administrator's Guide*

F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3).*F-Secure SSH2.0 for Windows NT and 95*

F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3).*F-Secure VPN+ Administrator's Guide*

F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6).*F-Secure VPN+ 4.1*

F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6).*F-Secure SSH*

F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6).*F-Secure SSH 2.0 for Windows NT and 95*

F-Secure, *F-Secure Evaluation Kit* (Sep. 1998) (FSECURE 00000009) (Evaluation Kit 9).*F-Secure Evaluation Kit*

F-Secure, *F-Secure SSH User's & , Administrator's Guide* (Sep. 1998) (from FSECURE 00000009) (SSH Guide 9).*F-Secure SSH User's Administrator's Guide*

F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sep. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9).*F-Secure SSH 2.0 for Windows NT and 95*

F-Secure, *F-Secure VPN+* (Sep. 1998) (from FSECURE 00000009) (VPN+ Guide 9).*F-Secure VPN+*

F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools).*F-Secure Management Tools, Administrator's Guide*

F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide).*F-Secure Desktop, User's Guide*

SafeNet, Inc., *VPN Policy Manager* (Jan. 2000) (VPN Policy Manager).*VPN Policy Manager*

F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+).

IRE, Inc., *SafeNet/Soft-PK Version 4* (Mar. 28, 2000) (Soft-PK Version 4).*SafeNet/Soft-PK Version 4*

IRE/SafeNet Inc., *VPN Technologies Overview* (Mar. 28, 2000) (Safenet VPN Overview).*VPN Technologies Overview*

IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (Jun. 22, 1999) (Safenet Addendum).*SafeNet / Security Center Technical Reference Addendum*

IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (Mar. 30, 2000) (VPN Policy Manager System Description).*System Description for VPN Policy Manager and SafeNet/SoftPK*

IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager).

IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager).*SafeNet/VPN Policy Manager Quick Start Guide Version 1*

Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (Jul. 22, 1996) (Gauntlet Functional Summary).*Gauntlet Internet Firewall, Firewall Product Functional Summary*

Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall).*Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0*

Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79.*Windows NT Terminal Server and Citrix Metaframe*

Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers).*Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame*

Bernard Aboba et al., *Securing L2TP using IPSEC* (Feb. 2, 1999).*Securing L2TP using IPSEC*

156. *Finding Your Way Through the VPN Maze* (1999) ("PGP").*Finding Your Way Through the VPN Maze*

Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview).

TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep").*The Business Case for Secure VPNs*

WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14, 2000).*WatchGuard LiveSecurity for MSS Powerpoint*

WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (Jul. 21, 2000).*MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes*

Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (, Contract No. F30602-98-C-0012*) (Jan. 29, 1998).*Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 Contract No. F30602-98-C-0012*

GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (, IFD) , 1.2 Report, Rev. 1.0* (Sep. 21, 1998).*DARPA Information Assurance Program Integrated Feasibility Demonstration IFD1.2 Report, Rev. 1.0*

BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (Mar. 16-Apr. 30, 1998).*TIS Labs Monthly Status Report*

DARPA, *Dynamic Virtual Private Network (, VPN) , Powerpoint.Dynamic Virtual Private Network VPNPowerpoint*

GTE Internetworking, *Contractor's Program Progress Report* (Mar. 16-Apr. 30, 1998).*Contractor's Program Progress Report*

Darrell Kindred, *Dynamic Virtual Private Networks (, DVPN) , Countermeasure Characterization* (Jan. 30, 2001).*Dynamic Virtual Private Networks DVPNCountermeasure Characterization*

Virtual Private Networking Countermeasure Characterization (Mar. 30, 2000).*Virtual Private Networking Countermeasure Characterization*

Virtual Private Network Demonstration (Mar. 21, 1998).*Virtual Private Network Demonstration*

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (, VPNs) , and Integrated Security Management* (2000).*Dynamic Virtual Private Networks VPNsand Integrated Security Management*

Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000).*Create/Add DVPN Enclave*

NAI Labs, *IFE 3.1 Integration Demo* (2000).*IFE 3.1 Integration Demo*

Information Assurance, *Science Fair Agenda* (2000).*Science Fair Agenda*

Darrell Kindred et al., *Proposed Threads for IFE 3.1* (Jan. 13, 2000).*Proposed Threads for IFE 3.1*

IFE 3.1 Technology Dependencies (2000).*IFE 3.1 Technology Dependencies*

IFE 3.1 Topology (Feb. 9, 2000).*IFE 3.1 Topology*

Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis* & *, Thread Development* (Jan. 10-11, 2000).*Information Assurance Integration: IFE 3.1, Hypothesis Thread Development*

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000).*Dynamic Virtual Private Networks Presentation*

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000).*Dynamic Virtual Private Networks Presentation v.2*

Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000).*Dynamic Virtual Private Networks Presentation v.3*

T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (Aug. 1, 1999) (VPNA).*Virtual Private Network Architecture*

Network Associates Products—*PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999).*PGP Total Network Security Suite, Dynamic Virtual Private Networks*

Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology).

David Johnson et. al., *A Guide to Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology).*A Guide to Microsoft Proxy Server 2.0*

Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology).*Setting Server Parameters*

Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology).*Microsoft Proxy Server 2*

Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology).*MCSE Proxy Server 2 Study Guide*

M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology).*IIS 4 and Proxy Server 2*

David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology).*MCSE Test Success: Proxy Server 2*

John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology).*The Windows NT and Windows 2000 Answer Book*

Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN).*Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0*

Network Associates *Gauntlet Firewall for UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN).*Gauntlet Firewall for UNIX Global Virtual Private Network User's Guide Version 5.0*

File History for U.S. Appl. No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date Aug. 31, 2000.

AutoSOCKS v2.1, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html.*AutoSOCKS v2.1*
Ran Atkinson, *Use of DNS to Distribute Keys*, Sep. 7, 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html.*Use of DNS to Distribute Keys*
FirstVPN Enterprise Networks, Overview.
Chapter 1: Introduction to Firewall Technology, Administration Guide; Dec. 19, 2007, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062.(—)(—)
The TLS Protocol Version 1.0; Jan. 1999; p. 65 of 71.
Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.
Virtual Private Networks—Assured Digital Incorporated—ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm.
Accessware—The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html.
Extended System Press Release, Sep. 2, 1997; *Extended VPN Uses the Internet to Create Virtual Private Networks*, www.extendedsystems.com.*Extended VPN Uses the Internet to Create Virtual Private Networks*
Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html.
Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sep. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com.
Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing.

CORE TERMS: packet, computer, server, network, message, router, sync, node, transmitter, destination, receiver, header, user, window, path, ckpt, layer, terminal, hopping, proxy, traffic, synchronization, domain, reqs, algorithm, internet, transmission, virtual, random, protocol

ENGLISH-ABST:

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

NO-OF-CLAIMS: 29

EXMPL-CLAIM: 2

NO-OF-FIGURES: 40

NO-DRWNG-PP: 40

PARENT-PAT-INFO:

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001]This application claims priority from and is a divisional patent application of U.S. application Ser. No. 09/558,209, filed Apr. 26, 2000 and now abandoned, which is in turn a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/504,783, filed on Feb. 15, 2000 and now U.S. Pat. No. 6,502,135, issued Dec. 31, 2002, which in turn claims priority from and is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999, now U.S. Pat. No. 7,010,604, issued Mar. 7, 2006. The subject matter of U.S. application Ser. No.

09/429,643, which is bodily incorporated herein, derives from provisional U.S. application No. 60/106,261 (filed Oct. 30, 1998) and Ser. No. 60/137,704 (filed Jun. 7, 1999). The present application is also related to U.S. application Ser. No. 09/558,210, filed Apr. 26, 2000 and now abandoned, which is incorporated by reference herein.

SUMMARY:

BACKGROUND OF THE INVENTION

[0002]A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal **100** and a destination terminal **110** are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal **100** may transmit secret information to terminal **110** over the Internet **107**. Also, it may be desired to prevent an eavesdropper from discovering that terminal **100** is in communication with terminal **110**. For example, if terminal **100** is a user and terminal **110** hosts a web site, terminal **100**'s user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

[0003]Data security is usually tackled using some form of data encryption. An encryption key **48** is known at both the originating and terminating terminals **100** and **110**. The keys may be private and public at the originating and destination terminals **100** and **110**, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

[0004]To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

[0005]To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

[0006]Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

[0007]ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

[0008]Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

[0009]A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

[0010]Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

[0011]Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet **140** undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called agile routing. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

[0012]The IP address of a TARP router can be changed, a feature called IP agility. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

[0013]The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

[0014]Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

[0015]To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IP $_{(T)}$are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

[0016]Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security. Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

[0017]Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

[0018]The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack.

Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

[0019]IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

[0020]As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

[0021]Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

[0022]In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

[0023]Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities

[0024]The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

[0025]According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer.

[0026]According to another aspect of the invention, a command is entered to define a setup parameter associated with the secure communication link mode of communication. Consequently, the secure communication mode is automatically established when a communication link is established over the computer network.

[0027]The present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network. A non-standard top-level domain name is then sent over the virtual private network communication to a predetermined computer network address, such as a computer network address for a secure domain name service (SDNS).

[0028]The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

[0029]The present invention provides a way to encapsulate existing application network traffic at the application layer of a client computer so that the client application can securely communicate with a server protected by an agile network protocol. The advantages of the present invention are provided by a method for communicating using a private communication link between a client computer and a server computer over a computer network, such as the Internet. According to the invention, an information packet is sent from the client computer to the server computer over the computer network. The information packet contains data that is inserted into the payload portion of the packet at the application layer of the client computer and is used for forming a virtual private connection between the client computer and the server computer. The modified information packet can be sent through a firewall before being sent over the computer network to the server computer and by working on top of existing protocols (i.e., UDP, ICMP and TCP), the present invention more easily penetrates the firewall. The information packet is received at a kernel layer of an operating system on the server side. It is then determined at the kernel layer of the operating system on the host computer whether the information packet contains the data that is used for forming the virtual private connection. The server side replies by sending an information packet to the client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet. Alternative, both information packets could be a

TCP/IP protocol information packet, or an ICMP protocol information packet.

DRWDESC:

BRIEF DESCRIPTION OF THE DRAWINGS

[0030]FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment.

[0031]FIG. 2 is an illustration of secure communications over the Internet according to a an embodiment of the invention.

[0032]FIG. 3*a* is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

[0033]FIG. 3*b* is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

[0034]FIG. 4 is an illustration of an OSI layer location of processes that may be used to implement the invention.

[0035]FIG. 5 is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

[0036]FIG. 6 is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

[0037]FIG. 7 is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

[0038]FIG. 8 shows how a secure session is established and synchronized between a client and a TARP router.

[0039]FIG. 9 shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

[0040]FIG. 10 shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

[0041]FIG. 11 shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

[0042]FIG. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

[0043]FIG. 12B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

[0044]FIG. 13 shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

[0045]FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

[0046]FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

[0047]FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

[0048]FIG. 17 shows a storage array for a receiver's active addresses.

[0049]FIG. 18 shows the receiver's storage array after receiving a sync request.

[0050]FIG. 19 shows the receiver's storage array after new addresses have been generated.

[0051]FIG. 20 shows a system employing distributed transmission paths.

[0052]FIG. 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

[0053]FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

[0054]FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

[0055]FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

[0056]FIG. 24 shows an example using the system of FIG. 23.

[0057]FIG. 25 shows a conventional domain-name look-up service.

[0058]FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

[0059]FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

[0060]FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

[0061]FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

[0062]FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

[0063]FIG. 31 shows a signaling server **3101** and a transport server **3102** used to establish a VPN with a client computer.

[0064]FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

[0065]FIG. 33 shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use.

[0066]FIG. 34 shows a flow diagram for installing and establishing a "one-click" secure communication link over a computer network according to the present invention.

[0067]FIG. 35 shows a flow diagram for registering a secure domain name according to the present invention.

[0068]FIG. 36 shows a system block diagram of a computer network in which a private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks.

[0069]FIG. 37 shows a flow diagram for establishing a virtual private connection that is encapsulated using an existing network protocol.

DETDESC:

DETAILED DESCRIPTION OF THE INVENTION

[0070]Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers **122-127** that are similar to regular IP routers **128-132** in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets **140**. TARP packets **140** are identical to normal IP packet messages that are routed by regular IP routers **128-132** because each TARP packet **140** contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's **140** IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal **110**. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet **140** since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal **110**.

[0071]Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key **146**. The link key **146** is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal **100** and the destination TARP terminal **110**. Each TARP router **122-127**, using the link key **146** it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key **146** and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

[0072]Once the outer layer of decryption is completed by a TARP router **122-127**, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet **140** to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet **140** to another TARP router **122-127** or to the destination TARP terminal **110**. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet **140** may forward the TARP packet **140** to the destination TARP terminal **110**. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet **140** may forward the TARP packet **140** to a TARP router **122-127** that the current TARP terminal chooses at random. As a result, each TARP packet **140** is routed through some minimum number of hops of TARP routers **122-127** which are chosen at random.

[0073]Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called agile routing. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

[0074]A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header $IP_{(C)}$. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

[0075]While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers **122**-**127** intervening between the originating **100** and destination **110** TARP terminals. The session key is used to decrypt the payloads of the TARP packets **140** permitting an entire message to be reconstructed.

[0076]In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets **140** may be used as desired.

[0077]Referring to FIG. 3*a*, to construct a series of TARP packets, a data stream **300** of IP packets **207***a*, **207***b*, **207***c*, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments **1**-**9** are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets **207**a-**207**c used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the interleave window.

[0078]To create a packet, the transmitting software interleaves the normal IP packets **207***a* et. seq. to form a new set of interleaved payload data **320**. This payload data **320** is then encrypted using a session key to form a set of session-key-encrypted payload data **330**, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets **207***a*-**207***c*, new TARP headers IP$_{(T)}$are formed. The TARP headers IP$_{(T)}$can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP$_{(T)}$are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

• -

o -

1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.

o -

2. An interleave sequence number—an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.

o -

3. A time-to-live (TTL) datum—indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.

o -

4. Data type identifier—indicates whether the payload contains, for example, TCP or UDP data.

o -

5. Sender's address—indicates the sender's address in the TARP network.

o -

6. Destination address—indicates the destination terminal's address in the TARP network.

7. Decoy/Real—an indicator of whether the packet contains real message data or dummy decoy data or a combination.

[0086]Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets **207***a*-**207***c* all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

[0087]Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

[0088]Referring to FIG. 3*b*, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block **520** for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. 3*b*. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of FIG. 3*a*. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. 3*a*. The remaining process is as shown in, and discussed with reference to, FIG. 3*a*.

[0089]Once the TARP packets **340** are formed, each entire TARP packet **340**, including the TARP header $IP_{(T)}$, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header $IP_{(C)}$is added to each encrypted TARP packet **340** to form a normal IP packet **360** that can be transmitted to a TARP router. Note that the process of constructing the TARP packet **360** does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

[0090]Note that, TARP header $IP_{(T)}$could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

[0091]The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. 4, a TARP transceiver **405** can be an originating terminal **100**, a destination terminal **110**, or a TARP router **122**-**127**. In each TARP Transceiver **405**, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver **405** is a router, the received TARP packets **140** are not processed into a stream of IP packets **415** because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal **110**. The intervening process, a "TARP Layer" **420**, could be combined with either the data link layer **430** or the Network layer **410**. In either case, it would intervene between the data link layer **430** so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer **410**. As an example of combining the TARP layer **420** with the data link layer **430**, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

[0092]Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

[0093]Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

[0094]As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

[0095]Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

[0096]As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

[0097]Decoy packets may be generated by each TARP terminal **100**, **110** or each router **122**-**127** on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal **110** may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

[0098]Referring to FIG. 5, the following particular steps may be employed in the above-described method for routing TARP packets.

• -

o -

S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

o -

S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.

o -

S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

o -

S4. If the packet is a decoy packet, the perishable decoy counter is incremented.

o -

S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.

o -

S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.

o -

S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.

o -

S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.

o -

S10. The TARP packet is encrypted using the memorized link key.

o -

S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

[0109]Referring to FIG. 6, the following particular steps may be employed in the above-described method for generating TARP packets.

- -
  - -

    S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.
  - -

    S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.
  - -

    S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.
  - -

    S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.
  - -

    S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.
  - -

    S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

[0116]Referring to FIG. 7, the following particular steps may be employed in the above-described method for receiving TARP packets.

- -
  - -

    S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
  - -

    S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.

- -

S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

- -

S44. If the packet is a decoy packet, the perishable decoy counter is incremented.

- -

S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.

- -

S46. The TARP packets are cached until all packets forming an interleave window are received.

- -

S47. Once all packets of an interleave window are received, the packets are deinterleaved.

- -

S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.

- -

S49. The decrypted block is then divided using the window sequence data and the $IP_{(T\ )}$ headers are converted into normal $IP_{(C\ )}$headers. The window sequence numbers are integrated in the $IP_{(C\ )}$headers.

- -

S50. The packets are then handed up to the IP layer processes.

1. Scalability Enhancements

[0127]The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

[0128]A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

[0129]The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

[0130]In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

[0131]Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

[0132]The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

[0133]When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

[0134]FIG. 8 shows how a client computer **801** and a TARP router **811** can establish a secure session. When client **801** seeks to establish an IHOP session with TARP router **811**, the client **801** sends "secure synchronization" request ("SSYN") packet **821** to the TARP router **811**. This SYN packet **821** contains the client's **801** authentication token, and may be sent to the router **811** in an encrypted format. The source and destination IP numbers on the packet **821** are the client's **801** current fixed IP address, and a "known" fixed IP address for the router **811**. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's **801** SSYN packet **821**, the router **811** responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") **822** to the client **801**. This SSYN ACK **822** will contain the transmit and receive hopblocks that the client **801** will use when communicating with the TARP router **811**. The client **801** will acknowledge the TARP router's **811** response packet **822** by generating an encrypted SSYN ACK ACK packet **823** which will be sent from the client's **801** fixed IP address and to the TARP router's **811** known fixed IP address. The client **801** will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet **824**, will be sent with the first [sender, receiver] IP pair in the client's transmit table **921** (FIG. 9), as specified in the transmit hopblock provided by the TARP router **811** in the SSYN ACK packet **822**. The TARP router **811** will respond to the SSI packet **824** with an SSI ACK packet **825**, which will be sent with the first [sender, receiver] IP pair in the TARP router's transmit table **923**. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client **801** and the TARP router **811** will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client **801** and TARP router **802** may re-establish the secure session by the procedure outlined in FIG. 8 and described above.

[0135]While the secure session is active, both the client **901** and TARP router **911** (FIG. 9) will maintain their respective transmit tables **921**, **923** and receive tables **922**, **924**, as provided by the TARP router during session synchronization **822**. It is important that the sequence of IP pairs in the client's transmit table **921** be identical to those in the TARP router's receive table **924**; similarly, the sequence of IP pairs in the client's receive table **922** must be identical to those in the router's transmit table **923**. This is required for the session synchronization to be maintained. The client **901** need maintain only one transmit table **921** and one receive table **922** during the course of the secure session. Each sequential packet sent by the client **901** will employ the next [send, receive] IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router **911** will expect each packet arriving from the client **901** to bear the next IP address pair shown in its receive table.

[0136]Since packets can arrive out of order, however, the router **911** can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router **911** to the client **901** are maintained in an identical manner; in particular, the router **911** will select the next IP address pair from its transmit table **923** when constructing a packet to send to the client **901**, and the client **901** will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

[0137]While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

[0138]While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link-based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the [sender, receiver] IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of FIG. 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

[0139]The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

[0140]Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

[0141]As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in FIG. 10, for example, client **1001** can establish three simultaneous sessions with each of three TARP routers provided by different ISPs **1011**, **1012**, **1013**. As an example, the client **1001** can use three different telephone lines **1021**, **1022**, **1023** to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of-service attacks and traffic monitoring.

2. Further Extensions

[0142]The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

[0143]Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

[0144]Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. 11, for example, a first Ethernet frame **1150** comprises a frame header **1101** and two embedded IP packets IPI and IP**2**, while a second Ethernet frame **1160** comprises a different frame header **1104** and a single IP packet IP**3**. Each frame header generally includes a source hardware address **1101**A and a destination hardware address **1101**B; other well-known fields in frame headers are omitted from FIG. 11 for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

[0145]It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

[0146]FIG. 12A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

[0147]As shown in FIG. 12A, two computer nodes **1201** and **1202** communicate over a communication channel such as an Ethernet. Each node executes one or more application programs **1203** and **1218** that communicate by transmitting packets through communication software **1204** and **1217**, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software **1204** and **1217** can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

[0148]The lowest levels of communication software **1204** and **1217** communicate with hardware components **1206** and **1214** respectively, each of which can include one or more registers **1207** and **1215** that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

[0149]One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

[0150]This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

[0151]Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

[0152]One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

[0153]In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if all of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

[0154]Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

[0155]Reference will now be made to FIGS. 12A and 12B in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes **1201** and **1202** are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (**1204** and **1217**, respectively) contains a modified element **1205** and **1216** that performs certain functions that deviate from the standard communication protocols. In particular, computer node **1201** implements a first "hop" algorithm **1208**X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node **1201** maintains a transmit table **1208** containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node **1202**. As each new IP packet is formed, the next sequential entry out of the sender's transmit table **1208** is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

[0156]At the receiving node **1202**, the same IP hop algorithm **1222**X is maintained and used to generate a receive table **1222** that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table **1208** matching the second five entries of receive table **1222**. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node **1202** maintains a receive window W**3** that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window W**3** slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window W**3** will be accepted; those falling outside of window W**3** will be rejected as invalid. The length of window W**3** can be adjusted as necessary to reflect network delays or other factors.

[0157]Node **1202** maintains a similar transmit table **1221** for creating IP packets and frames destined for node **1201** using a potentially different hopping algorithm **1221**X, and node **1201** maintains a matching receive table **1209** using the same algorithm **1209**X. As node **1202** transmits packets to node **1201** using seemingly random IP source, IP destination, and/or discriminator fields, node **1201** matches the incoming packet values to those falling within window WI maintained in its receive table. In effect, transmit table **1208** of node **1201** is synchronized (i.e., entries are selected in the same order) to receive table **1222** of receiving node **1202**. Similarly, transmit table **1221** of node **1202** is synchronized to receive table **1209** of node **1201**. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

[0158]In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node **1201** further maintains a transmit table **1210** using a transmit algorithm **1210**X to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields **1101**A and **1101**B in FIG. 11) that are synchronized to a corresponding receive table **1224** at node **1202**. Similarly, node **1202** maintains a different transmit table **1223** containing source and destination hardware addresses that is synchronized with a corresponding receive table **1211** at node **1201**. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

[0159]FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

[0160]In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

[0161]In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. 12A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

[0162]Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

[0163]Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

[0164]It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

[0165]One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

[0166]A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

[0167]In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

[0168]In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

[0169]Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair—and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

[0170]The aforementioned scheme may have some inherent security issues associated with it—namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

[0171]A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

[0172]Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

[0173]One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. 13, where (for example) a first ISP **1302** is the sender and a second ISP **1303** is the receiver. (Other alternatives are possible from FIG. 13.) A transmitted packet comprises a public or "outer" header **1305** that is not encrypted, and a private or "inner" header **1306** that is encrypted using for example a link key. Outer header **1305** includes a public sync portion while inner header **1306** contains the private sync portion. A receiving node decrypts the inner header using a decryption function **1307** in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step **1308**.) The public and decrypted private sync portions are combined in function **1308** in order to generate the combined sync **1309**. The combined sync (**1309**) is then fed into the RNG (**1310**) and compared to the IP address pair (**1311**) to validate or reject the packet.

[0174]An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent—even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

[0175]In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

[0176]The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

[0177]As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

[0178]A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

- -
    - -

      1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
    - -

      2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized. According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):
    - -

      1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
    - -

      2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and

a new ckpt_r to be generated.

o -

3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14). When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

[0184]Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack , at which point transmission is reestablished.

[0185]From the receiver's perspective, the scheme operates as follows: (1) when it receives a sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

[0186]If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it will actually help to re-establish synchronization.

[0187]A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead Capability

[0188]An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

[0189]Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead n steps efficiently. An LCR generates random numbers $X_{(1)}$, $X_{(2)}$, $X_{(3\ )}$. . . $X_{(k\ )}$starting with seed $X_{(0\ )}$using a recurrence $X_{(1)}=(a\ X_{(i\&minus;1)}$ $+b)$ mod c,   (1) where a, b and c define a particular LCR. Another expression for $X_{(i)}$, $X_{(i)}$ $=((a^{(i)}(X_{(0)}+b)\&minus;b)/(a\&minus;1))$ mod c (2) enables the jump-ahead capability. The factor $a^{(i\ )}$can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as: $X_{(i)}$=($a^{(i)}$($X_{(0)}$(a&minus;1)+b)&minus;b)/(a&minus;1) mod c.   (3) It can be shown that: ($a^{(i)}$($X_{(0)}$(a&minus;1)+b)&minus;b)/(a&minus;1) mod c=(($a^{(i\ )}$ mod((a&minus;1)c)($X_{(0)}$(a&minus;1)+b)&minus;b)/(a&minus;1)) mod c   (4). ($X_{(0)}$ (a&minus;1)+b) can be stored as ($X_{(0)}$(a&minus;1)+b) mod c, b as b mod c and compute $a^{(i\ )}$mod ((a&minus;1)c) (this requires O(log(i)) steps).

[0190]A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every n packets. The window would commence n IP pairs from the start of the previous window. Using $X_{(j)}^{(w)}$, the random number at the $j^{(th\ )}$checkpoint, as $X_{(0\ )}$and n as i, a node can store $a^{(n\ )}$mod((a&minus;1)c) once per LCR and set $X_{(j+1)}^{(w)}$=$X_{(n(j+1))}$= (($a^{(n\ )}$mod((a&minus;1)c)($X_{(j)}^{(w)}$(a&minus;1)+b)&minus;b)/(a&minus;1))mod c,   (5) to generate the random number for the $j+1^{(th\ )}$synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n). Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

[0191]Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack-against the encryptor.

F. Random Number Generator Example

[0192]Consider a RNG where a=31, b=4 and c=15. For this case equation (1) becomes: $X_{(i)}$=(31 $X_{(i\&minus;1)}$+4) mod 15.   (6)

[0193]If one sets $X_{(0)}$=1, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a^{(n)}$ =313=29791, c*(a&minus;1)=15*30=450 and $a^{(n\ )}$mod((a&minus;1)c)=$31^{(3)}$mod(15*30)=29791 mod (450)=91. Equation (5) becomes: ((91($X_{(i)}$30+4)&minus;4)/30)mod 15   (7). Table 1 shows the jump ahead calculations from (7). The calculations start at 5 and jump ahead 3.

[0194]

Search terms may have been found within the contents of this table. Please see the table in the original document.

G. Fast Packet Filter

[0195]Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

[0196]Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

- -

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.

- -

2. There are $2^{(24)}$(~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).

- -

3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

[0200]The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B-trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

[0201]A presence vector is a bit vector of length $2^{(n)}$that can be indexed by n-bit numbers (each ranging from 0 to $2^{(n)}$&minus;1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the $x^{(th)}$bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a **1**, which will be referred to as the "test."

[0202]For example, suppose one wanted to represent the number 135 using a presence vector. The 135$^{(th)}$bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135$^{(th)}$bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

[0203]There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

[0204]A presence vector will have a 1 in the y$^{(th\ )}$bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

[0205]Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

[0206]The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

I. Further Synchronization Enhancements

[0207]A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2&times;WINDOW_SIZE+OoO active addresses (1&lE;OoO&lE;WINDOW_SIZE and WINDOW_SIZE&gE;1). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver's active addresses.

[0208]The receiver starts with the first 2&times;WINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as "used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last initial transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. 18 when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

[0209]FIG. 19 shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2&times;WINDOW_SIZE&minus;OoO then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

- -

  1. There is no need for an efficient jump ahead in the random number generator,
- -

  2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
- -

  3. No timer based re-synchronization is necessary. This is a consequence of 2.
- -

  4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

[0214]Another embodiment incorporating various inventive principles is shown in FIG. 20. In this embodiment, a message transmission system includes a first computer **2001** in communication with a second computer **2002** through a network **2011** of intermediary computers. In one variant of this embodiment, the network includes two edge routers **2003** and **2004** each of which is linked to a plurality of Internet Service Providers (ISPs) **2005** through **2010**. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. 20, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. 20 to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element **2005**) to ISP D (element **2008**)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

[0215]As shown in FIG. 21, computer **2001** or edge router **2003** incorporates a plurality of link transmission tables **2100** that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table **2101** contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer **2001** to second computer **2002**, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element **2005**) and ISP B (element **2008**)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link table can be set to a "down" condition as shown in table **2105**, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. Continuation-in-Part Improvements

[0216]The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities. Each is discussed separately below.

A. Load Balancer

[0217]Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. 20 and 21 and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

[0218]In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

[0219]When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

[0220]Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

[0221]According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

[0222]Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

[0223]The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

[0224]FIG. 22A shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. 22A. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

[0225]Beginning in step **2201**, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

[0226]In step **2202**, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step **2201**.

[0227]In step **2203**, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step **2207** a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step **2209** the weight is set to the minimum level and processing resumes at step **2201**. If the weight is above the minimum level, then in step **2208** the weight is gradually decreased for the path, then in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

[0228]If in step **2203** the quality of the path was greater than or equal to the threshold, then in step **2204** a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step **2205** the weight is increased toward the steady-state value, and in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step **2204** the weight is not less than the steady-state value, then processing resumes at step **2201** without adjusting the weights.

[0229]The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

[0230]Although not explicitly shown in FIG. 22A the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

[0231]Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

[0232]FIG. 22B shows steps that can be executed to shut down transmission links where a transmitter turns off. In step **2210**, a transmitter shut-down event occurs. In step **2211**, a test is made to determine whether at least one transmitter is still turned on. If not, then in step **2215** all packets are dropped until a transmitter turns on. If in step **2211** at least one transmitter is turned on, then in step **2212** the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

[0233]FIG. 23 shows a computer node **2301** employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23, four transmission paths X**1** through X**4** are defined for communicating between the two nodes. Each node includes a packet transmitter **2302** that operates in accordance with a transmit table **2308** as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver **2303** that operates in accordance with a receive table **2309**, including a moving window W that moves as valid packets are received. Invalid packets having source and destination addresses that do not fall within window W are rejected.

[0234]As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table **2308** according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch **2307**. Switch **2307**, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table **2306**. For example, if the weight for path X**1** is 0.2, then every fifth packet will be transmitted on path X**1**. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

[0235]Packet receiver **2303** generates an output to a link quality measurement function **2304** that operates as described above to determine the quality of each transmission path. (The input to packet receiver **2303** for receiving incoming packets is omitted for clarity). Link quality measurement function **2304** compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function **2305**. If a weight adjustment is required, then the weights in table **2306** are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

[0236]Link quality measurement function **2304** can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function **2304**. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This allows the transmitter to compare messages sent to messages received in order to assess the health of the link.

[0237]If synchronization is completely lost, weight adjustment function **2305** decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

[0238]When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

[0239]1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to: *P*&prime;=α&times;MIN+(1&minus;α)&times;*P*   (1) Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

[0240]2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to: *P&prime;=β&times;S+* (1&minus;β)&times;*P*   (2) where β is a parameter such that 0<=β<=1 that determines the damping rate of P.

[0241]Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

[0242]A detailed example will now be provided with reference to FIG. 24. As shown in FIG. 24, a first computer **2401** communicates with a second computer **2402** through two routers **2403** and **2404**. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

[0243]Suppose that a first link L**1** can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L**2** can sustain 75 Mb/s and has a window size of 24; and link L**3** can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200 Mb/s. The steady state traffic weights are 0.5 for link L**1**; 0.375 for link L**2**, and 0.125 for link L**3**. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, α=0.75 and β=0.5. These traffic weights will remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

[0244]1. Link L**1** receives a SYNC_ACK containing a MESS_R of **24**, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link **1** would be below THRESH (0.8). Consequently, link L**1**'s traffic weight value would be reduced to 0.12825, while link L**2**'s traffic weight value would be increased to 0.65812 and link L**3**'s traffic weight value would be increased to 0.217938.

[0245]2. Link L**2** and L**3** remained healthy and link L**1** stopped to synchronize. Then link L**1**'s traffic weight value would be set to 0, link L**2**'s traffic weight value would be set to 0.75, and link L**33**'s traffic weight value would be set to 0.25.

[0246]3. Link L**1** finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the

MESS_T (32) messages transmitted in the last window were successfully received. Link **L1** would be below THRESH. Link **L1**'s traffic weight value would be increased to 0.005, link **L2**'s traffic weight value would be decreased to 0.74625, and link **L3**'s traffic weight value would be decreased to 0.24875.

[0247]4. Link **L1** received a SYNC_ACK containing a MESS_R of **32** indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link **L1** would be above THRESH. Link **L1**'s traffic weight value would be increased to 0.2525, while link **L2**'s traffic weight value would be decreased to 0.560625 and link **L3**'s traffic weight value would be decreased to 0.186875.

[0248]5. Link **L1** received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link **L1** would be above THRESH. Link **L1**'s traffic weight value would be increased to 0.37625; link **L2**'s traffic weight value would be decreased to 0.4678125, and link **L3**'s traffic weight value would be decreased to 0.1559375.

[0249]6. Link **L1** remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

[0250]A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

[0251]Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

[0252]This conventional scheme is shown in FIG. 25. A user's computer **2501** includes a client application **2504** (for example, a web browser) and an IP protocol stack **2505**. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack **2505**) to a DNS **2502** to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application **2504**, which is then able to use the IP address to communicate with the host **2503** through separate transactions such as PAGE REQ and PAGE RESP.

[0253]In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

[0254]One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

[0255]The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

[0256]According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

[0257]FIG. 26 shows a system employing various principles summarized above. A user's computer **2601** includes a conventional client (e.g., a web browser) **2605** and an IP protocol stack **2606** that preferably operates in accordance with an IP hopping function **2607** as outlined above. A modified DNS server **2602** includes a conventional DNS server function **2609** and a DNS proxy **2610**. A gatekeeper server **2603** is interposed between the modified DNS server and a secure target site **2704**. An "unsecure" target site **2611** is also accessible via conventional IP protocols.

[0258]According to one embodiment, DNS proxy **2610** intercepts all DNS lookup functions from client **2605** and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy **2610** determines whether the user has sufficient security privileges to access the site. If so, DNS proxy **2610** transmits a message to gatekeeper **2603** requesting that a virtual private network be created between user computer **2601** and secure target site **2604**. In one embodiment, gatekeeper **2603** creates "hopblocks" to be used by computer **2601** and secure target site **2604** for secure communication. Then, gatekeeper **2603** communicates these to user computer **2601**. Thereafter, DNS proxy **2610** returns to user computer **2601** the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) **2604**, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

[0259]Had the user requested lookup of a non-secure web site such as site **2611**, DNS proxy would merely pass through to conventional DNS server **2609** the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site **2611**. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy **2610** would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

[0260]Gatekeeper **2603** can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server **2602**. In general, it is anticipated that gatekeeper **2703** facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site **2604** are assumed to be equipped with a secure communication function such as an IP hopping function **2608**.

[0261]It will be appreciated that the functions of DNS proxy **2610** and DNS server **2609** can be combined into a single server for convenience. Moreover, although element **2602** is shown as combining the functions of two servers, the two servers can be made to operate independently.

[0262]FIG. 27 shows steps that can be executed by DNS proxy server **2610** to handle requests for DNS look-up for secure hosts. In step **2701**, a DNS look-up request is received for a target host. In step **2702**, a check is made to determine whether access to a secure host was requested. If not, then in step **2703** the DNS request is passed to conventional DNS server **2609**, which looks up the IP address of the target site and returns it to the user's application for further processing.

[0263]In step **2702**, if access to a secure host was requested, then in step **2704** a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper **2603** (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

[0264]If the user is not authorized to access the secure site, then a "host unknown" message is returned (step **2705**). If the user has sufficient security privileges, then in step **2706** a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

[0265]Some or all of the security functions can be embedded in gatekeeper **2603**, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy **2610** communicates with gatekeeper **2603** to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:

[0266]Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

[0267]Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would reject the request, informing DNS proxy server **2610** that it was unable to find the target computer. The DNS proxy **2610** would then return a "host unknown" error message to the client.

[0268]Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server **2610**, which would check its rules and determine that no VPN is needed. Gatekeeper **2603** would then inform the DNS proxy server to forward the request to conventional DNS server **2609**, which would resolve the request and return the result to the DNS proxy server and then back to the client.

[0269]Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper **2603**. Gatekeeper **2603** would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server **2610** to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

[0270]One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

[0271]In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. 28, suppose that a first host computer **2801** is communicating with a second host computer **2804** using the IP address hopping principles described above. The first host computer is coupled through an edge router **2802** to an Internet Service Provider (ISP) **2803** through a low bandwidth link (LOW BW), and is in turn coupled to second host computer **2804** through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router **2802**.

[0272]Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer **2801** across high bandwidth link HIGH BW. Normally, host computer **2801** would be able to quickly reject the packets since they would not fall within the acceptance window permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer **2801**. Consequently, the link to host computer **2801** is effectively flooded before the packets can be discarded.

[0273]According to one inventive improvement, a "link guard" function **2805** is inserted into the high-bandwidth node (e.g., ISP **2803**) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

[0274]In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc **2401**], the packets have IP protocols **420** and **421**. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, **2805**, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid. According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP **2903** maintains a copy **2910** of the receive table used by host computer **2901**. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard **2805** validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc **2104**].

[0275]According to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

[0276]As shown in FIG. 29, for example, suppose that a first host computer **2900** is communicating with a second host computer **2902** over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP **2901** and a low bandwidth link LOW BW through an edge router **2904**. In accordance with the basic architecture described above, first host computer **2900** and second host computer **2902** would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables **2905**, **2906**, **2912** and **2913**. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

[0277]Suppose that a nefarious computer hacker **2903** was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP **2901**, and that these packets are being forwarded over a low-bandwidth link. Hacker computer **2903** could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer **3000** would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard **2911** would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

[0278]According to one embodiment of the improvement, ISP **2901** maintains a separate VPN with first host computer **2900**, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer **2900**. The cryptographic keys used to authenticate VPN packets at the link guard **2911** and the cryptographic keys used to encrypt and decrypt the VPN packets at host **2902** and host **2901** can be different, so that link guard **2911** does not have access to the private host data; it only has the capability to authenticate those packets.

[0279]According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard **2911** can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

[0280]In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively control the rate at which its hopping window moves by delaying "SYNC ACK" responses to "SYNC_REQ" messages.

[0281]A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT_N. It is a simple matter of deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

[0282]Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

[0283]In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate, each receiver could defer issuing a new CKPT_N until M&times;N&times;W/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will re-issue the SYNC_REQ every T**1** seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

[0284]Two practical issues should be considered when implementing the above scheme:

[0285]1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

[0286]2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing for a period (e.g. the network dropping a SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

[0287]To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of M&times;N&times;W/R seconds after the last SYNC_REQ has been received and accepted, 2&times;M&times;N&times;W/R seconds after next to the last SYNC_REQ has been received and accepted, C&times;M&times;N&times;W/R seconds after (C&minus;1)$^{(th\ )}$to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

[0288]FIG. 30 shows a system employing the above-described principles. In FIG. 30, two computers **3000** and **3001** are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer **3000** will be referred to as the receiving computer and computer **3001** will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver **3000**.

[0289]As described above, receiving computer **3000** maintains a receive table **3002** including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer **3001** maintains a transmit table **3003** from which the next IP address pairs will be selected when transmitting a packet to receiving computer **3000**. (For the sake of illustration, window W is also illustrated with reference to transmit table **3003**). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function **3010**. This is a request to receiver **3000** to synchronize the receive table **3002**, from which transmitter **3001** expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer **3001** transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver **3000** will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter **3001** will be discarded).

[0290]In accordance with the improvements described above, receiving computer **3000** performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. 30. In step **3004**, receiving computer **3000** receives the SYNC_REQ message. In step **3005**, a check is made to determine whether the request is a duplicate. If so, it is discarded in step **3006**. In step **3007**, a check is made to determine whether the SYNC_REQ received from transmitter **3001** was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step **3008** the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

[0291]Otherwise, if the rate has not been exceeded, then in step **3109** the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from the transmitter **3101**. Transmitter **3101** then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

[0292]In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

[0293]One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

[0294]FIG. 31 shows a system employing certain of the above-described principles. In FIG. 31, a signaling server **3101** and a transport server **3102** communicate over a link. Signaling server **3101** contains a large number of small tables **3106** and **3107** that contain enough information to authenticate a communication request with one or more clients **3103** and **3104**. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server **3102**, which is preferably a separate computer in communication with signaling server **3101**, contains a smaller number of larger hopping tables **3108**, **3109**, and **3110** that can be allocated to create a VPN with one of the client computers.

[0295]According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server **3101** will quickly reject invalid packets from unauthorized computers such as hacker computer **3105**. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server **3101** with bogus packets. Details of this scheme are provided below.

[0296]Signaling server **3101** receives the request **3111** and uses it to determine that client **3103** is a validly registered user. Next, signaling server **3101** issues a request to transport server **3102** to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client **3103**. The allocated hopping parameters are returned to signaling server **3101** (path **3113**), which then supplies the hopping parameters to client **3103** via path **3114**, preferably in encrypted form.

[0297]Thereafter, client **3103** communicates with transport server **3102** using the normal hopping techniques described above. It will be appreciated that although signaling server **3101** and transport server **3102** are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. 31 differently from as shown without departing from the inventive principles.

[0298]One advantage of the above-described architecture is that signaling server **3101** need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer **3105**. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server **3102**, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server **3102** or signaling server **3101**.

[0299]A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

[0300]The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element **3106** in FIG. 31.

[0301]The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

[0302]The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

[0303]Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

[0304]1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer Ti noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.

[0305]2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and other information (i.e., user credentials) contained in the inner header It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

[0306]3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.

[0307]4. T**1** expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer Ti noting CKPT_O again, and a SYNC REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.

[0308]5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

[0309]6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

[0310]FIG. 32 shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

[0311]Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

[0312]There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

[0313]The above-described procedures allow a client to be authenticated at signaling server **3201** while maintaining the ability of signaling server **3201** to quickly reject invalid packets, such as might be generated by hacker computer **3205**. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

F. One-Click Secure On-line Communications and Secure Domain Name Service

[0314]The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram **3300** of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer **3301**, such as a personal computer (PC), is connected to a computer network **3302**, such as the Internet, through an ISP **3303**. Alternatively, computer **3301** can be connected to computer network **3302** through an edge router. Computer **3301** includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer **3301** can communicate conventionally with another computer **3304** connected to computer network **3302** over a communication link **3305** using a browser **3306** that is installed and operates on computer **3301** in a well-known manner.

[0315]Computer **3304** can be, for example, a server computer that is used for conducting e-commerce. In the situation when computer network **3302** is the Internet, computer **3304** typically will have a standard top-level domain name such as .com, .net, .org, .edu, .mil or .gov.

[0316]FIG. 34 shows a flow diagram **3400** for installing and establishing a "one-click" secure communication link over a computer network according to the present invention. At step **3401**, computer **3301** is connected to server computer **3304** over a non-VPN communication link **3305**. Web browser **3306** displays a web page associated with server **3304** in a well-known manner. According to one variation of the invention, the display of computer **3301** contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network **3302** between terminal **3301** and server **3304**. Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer **3304**, thereby indicating that the entity providing server **3304** also provides VPN capability.

[0317]By displaying the "go secure" hyperlink, a user at computer **3301** is informed that the current communication link between computer **3301** and server computer **3304** is a non-secure, non-VPN communication link. At step **3402**, it is determined whether a user of computer **3301** has selected the "go secure" hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step **3402**, it is determined that the user has selected the "go secure" hyperlink, flow continues to step **3403** where an object associated with the hyperlink determines whether a VPN communication software module has already been installed on computer **3301**. Alternatively, a user can enter a command into computer **3301** to "go secure."

[0318]If, at step **3403**, the object determines that the software module has been installed, flow continues to step **3407**. If, at step **3403**, the object determines that the software module has not been installed, flow continues to step **3404** where a non-VPN communication link **3307** is launched between computer **3301** and a website **3308** over computer network **3302** in a well-known manner. Website **3308** is accessible by all computer terminals connected to computer network **3302** through a non-VPN communication link. Once connected to website **3308**, a software module for establishing a secure communication link over computer network **3302** can be downloaded and installed. Flow continues to step **3405** where, after computer **3301** connects to website **3308**, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal **3301** as software module **3309**. At step **3405**, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network **3302**. At step **3406**, the -communication link between computer **3301** and website **3308** is then terminated in a well-known manner.

[0319]By clicking on the "go secure" hyperlink, a user at computer **3301** has enabled a secure communication mode of communication between computer **3301** and server computer **3304**. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer **3301** and server computer **3304** are performed transparently to a user at computer **3301**.

[0320]At step **3407**, a secure VPN communications mode of operation has been enabled and software module **3309** begins to establish a VPN communication link. In one embodiment, software module **3309** automatically replaces the top-level domain name for server **3304** within browser **3406** with a secure top-level domain name for server computer **3304**. For example, if the top-level domain name for server **3304** is .com, software module **3309** replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module **3409** can replace the top-level domain name of server **3304** with any other non-standard top-level domain name.

[0321]Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module **3409** contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module **3309** accesses a secure portal **3310** that interfaces a secure network **3311** to computer network **3302**. Secure network **3311** includes an internal router **3312**, a secure domain name service (SDNS) **3313**, a VPN gatekeeper **3314** and a secure proxy **3315**. The secure network can include other network services, such as e-mail **3316**, a plurality of chatrooms (of which only one chatroom **3317** is shown), and a standard domain name service (STD DNS) **3318**. Of course, secure network **3311** can include other resources and services that are not shown in FIG. 33.

[0322]When software module **3309** replaces the standard top-level domain name for server **3304** with the secure top-level domain name, software module **3309** sends a query to SDNS **3313** at step **3408** through secure portal **3310** preferably using an administrative VPN communication link **3319**. In this configuration, secure portal **3310** can only be accessed using a VPN communication link. Preferably, such a VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence; an IP address hopping regime that pseudorandomly changes IP addresses in packets transmitted between a client computer and a secure target computer; periodically changing at least one field in a series of data packets according to a known sequence; an Internet Protocol (IP) address in a header of each data packet that is compared to a table of valid IP addresses maintained in a table in the second computer; and/or a comparison of the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window. Other types of VPNs can alternatively be used. Secure portal **3310** authenticates the query from software module **3309** based on the particular information hopping technique used for VPN communication link **3319**.

[0323]SDNS **3313** contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS **3313** stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS **3313** so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website. Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure securities trading website. When a user queries SDNS **3313** for the secure computer network address for the securities trading website, SDNS **3313** determines the particular secure computer network address based on the user's identity and the user's subscription level.

[0324]At step **3409**, SDNS **3313** accesses VPN gatekeeper **3314** for establishing a VPN communication link between software module **3309** and secure server **3320**. Server **3320** can only be accessed through a VPN communication link. VPN gatekeeper **3314** provisions computer **3301** and secure web server computer **3320**, or a secure edge router for server computer **3320**, thereby creating the VPN. Secure server computer **3320** can be a separate server computer from server computer **3304**, or can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer **3322**. Returning to FIG. 34, in step **3410**, SDNS **3313** returns a secure URL to software module **3309** for the scom server address for a secure server **3320** corresponding to server **3304**.

[0325]Alternatively, SDNS **3313** can be accessed through secure portal **3310** "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal **3310** preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS **3319**. Because the initial communication link in this situation is not a VPN communication link, the reply to the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS **3313** can be in the clear, and SDNS **3313** and gatekeeper **3314** can operate to establish a VPN communication link to the querying computer for sending the reply.

[0326]At step **3411**, software module **3309** accesses secure server **3320** through VPN communication link **3321** based on the VPN resources allocated by VPN gatekeeper **3314**. At step **3412**, web browser **3306** displays a secure icon indicating that the current communication link to server **3320** is a secure VPN communication link. Further communication between computers **3301** and **3320** occurs via the VPN, e.g., using a "hopping" regime as discussed above. When VPN link **3321** is terminated at step **3413**, flow continues to step **3414** where software module **3309** automatically replaces the secure top-level domain name with the corresponding non-secure top-level domain name for server **3304**. Browser **3306** accesses a standard DNS **3325** for obtaining the non-secure URL for server **3304**. Browser **3306** then connects to server **3304** in a well-known manner. At step **3415**, browser **3306** displays the "go secure" hyperlink or icon for selecting a VPN communication link between terminal **3301** and server **3304**. By again displaying the "go secure" hyperlink, a user is informed that the current communication link is a non-secure, non-VPN communication link.

[0327]When software module **3309** is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network **3302** are secure communication links. Thus, anytime that a communication link is established, the link is a VPN link. Consequently, software module **3309** transparently accesses SDNS **3313** for obtaining the URL for a selected secure website. In other words, in one embodiment, the user need not "click" on the secure option each time secure communication is to be effected.

[0328]Additionally, a user at computer **3301** can optionally select a secure communication link through proxy computer **3315**. Accordingly, computer **3301** can establish a VPN communication link **3323** with secure server computer **3320** through proxy computer **3315**. Alternatively, computer **3301** can establish a non-VPN communication link **3324** to a non-secure website, such as non-secure server computer **3304**.

[0329]FIG. 35 shows a flow diagram **3500** for registering a secure domain name according to the present invention. At step **3501**, a requester accesses website **3308** and logs into a secure domain name registry service that is available through website **3308**. At step **3502**, the requestor completes an online registration form for registering a secure domain name having a top-level domain name, such as .com, .net, .org, .edu, .mil or .gov. Of course, other secure top-level domain names can also be used. Preferably, the requestor must have previously registered a non-secure domain name corresponding to the equivalent secure domain name that is being requested. For example, a requestor attempting to register secure domain name "website.scom" must have previously registered the corresponding non-secure domain name "website.com".

[0330]At step **3503**, the secure domain name registry service at website **3308** queries a non-secure domain name server database, such as standard DNS **3322**, using, for example, a whois query, for determining ownership information relating to the non-secure domain name corresponding to the requested secure domain name. At step **3504**, the secure domain name registry service at website

3308 receives a reply from standard DNS **3322** and at step **3505** determines whether there is conflicting ownership information for the corresponding non-secure domain name. If there is no conflicting ownership information, flow continues to step **3507**, otherwise flow continues to step **3506** where the requestor is informed of the conflicting ownership information. Flow returns to step **3502**.

[0331]When there is no conflicting ownership information at step **3505**, the secure domain name registry service (website **3308**) informs the requester that there is no conflicting ownership information and prompts the requestor to verify the information entered into the online form and select an approved form of payment. After confirmation of the entered information and appropriate payment information, flow continues to step **3508** where the newly registered secure domain name sent to SDNS **3313** over communication link **3326**.

[0332]If, at step **3505**, the requested secure domain name does not have a corresponding equivalent non-secure domain name, the present invention informs the requestor of the situation and prompts the requestor for acquiring the corresponding equivalent non-secure domain name for an increased fee. By accepting the offer, the present invention automatically registers the corresponding equivalent non-secure domain name with standard DNS **3325** in a well-known manner. Flow then continues to step **3508**.

G. Tunneling Secure Address Hopping Protocol through Existing Protocol Using Web Proxy

[0333]The present invention also provides a technique for implementing the field hopping schemes described above in an application program on the client side of a firewall between two computer networks, and in the network stack on the server side of the firewall. The present invention uses a new secure connectionless protocol that provides good denial of service rejection capabilities by layering the new protocol on top of an existing IP protocol, such as the ICMP, UDP or TCP protocols. Thus, this aspect of the present invention does not require changes in the Internet infrastructure.

[0334]According to the invention, communications are protected by a client-side proxy application program that accepts unencrypted, unprotected communication packets from a local browser application. The client-side proxy application program tunnels the unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side. Of course, the unencrypted, unprotected communication packets can be encrypted prior to tunneling.

[0335]The client-side proxy application program is not an operating system extension and does not involve any modifications to the operating system network stack and drivers. Consequently, the client is easier to install, remove and support in comparison to a VPN. Moreover, the client-side proxy application can be allowed through a corporate firewall using a much smaller "hole" in the firewall and is less of a security risk in comparison to allowing a protocol layer VPN through a corporate firewall.

[0336]The server-side implementation of the present invention authenticates valid field-hopped packets as valid or invalid very early in the server packet processing, similar to a standard virtual private network, for greatly minimizing the impact of a denial of service attempt in comparison to normal TCP/IP and HTTP communications, thereby protecting the server from invalid communications.

[0337]FIG. 36 shows a system block diagram of a computer network **3600** in which a virtual private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks. FIG. 37 shows a flow diagram **3700** for establishing a virtual private connection that is encapsulated using an existing network protocol.

[0338]In FIG. 36 a local area network (LAN) **3601** is connected to another computer network **3602**, such as the Internet, through a firewall arrangement **3603**. Firewall arrangement operates in a well-known manner to interface LAN **3601** to computer network **3602** and to protect LAN **3601** from attacks initiated outside of LAN **3601**.

[0339]A client computer **3604** is connected to LAN **3601** in a well-known manner. Client computer **3604** includes an operating system **3605** and a web browser **3606**. Operating system **3605** provides kernel mode functions for operating client computer **3604**. Browser **3606** is an application program for accessing computer network resources connected to LAN **3601** and computer network **3602** in a well-known manner. According to the present invention, a proxy application **3607** is also stored on client computer **3604** and operates at an application layer in conjunction with browser **3606**. Proxy application **3607** operates at the application layer within client computer **3604** and when enabled, modifies unprotected, unencrypted message packets generated by browser **3606** by inserting data into the message packets that are used for forming a virtual private connection between client computer **3604** and a server computer connected to LAN **3601** or computer network **3602**. According to the invention, a virtual private connection does not provide the same level of security to the client computer as a virtual private network. A virtual private connection can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service that can be subscribed to by a user.

[0340]Proxy application **3607** is conveniently installed and uninstalled by a user because proxy application **3607** operates at the application layer within client computer **3604**. On installation, proxy application **3607** preferably configures browser **3606** to use proxy application for all web communications. That is, the payload portion of all message packets is modified with the data for forming a virtual private connection between client computer **3604** and a server computer. Preferably, the data for forming the virtual private connection contains field-hopping data, such as described above in connection with VPNs. Also, the modified message packets preferably conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol. Alternatively, proxy application **3606** can be selected and enabled through, for example, an option provided by browser **3606**. Additionally, proxy application **3607** can be enabled so that only the payload portion of specially designated message packets is modified with the data for forming a virtual private connection between client computer **3604** and a designated host computer. Specially designated message packets can be, for example, selected predetermined domain names.

[0341]Referring to FIG. 37, at step **3701**, unprotected and unencrypted message packets are generated by browser **3606**. At step **3702**, proxy application **3607** modifies the payload portion of all message packets by tunneling the data for forming a virtual private connection between client computer **3604** and a destination server computer into the payload portion. At step, **3703**, the modified message packets are sent from client computer **3604** to, for example, website (server computer) **3608** over computer network **3602**.

[0342]Website **3608** includes a VPN guard portion **3609**, a server proxy portion **3610** and a web server portion **3611**. VPN guard portion **3609** is embedded within the kernel layer of the operating system of website **3608** so that large bandwidth attacks on website **3608** are rapidly rejected. When client computer **3604** initiates an authenticated connection to website **3608**, VPN guard portion **3609** is keyed with the hopping sequence contained in the message packets from client computer **3604**, thereby performing a strong authentication of the client packet streams entering website **3608** at step **3704**. VPN guard portion **3609** can be configured for providing different levels of authentication and, hence, quality of service, depending upon a subscribed level of service. That is, VPN guard portion **3609** can be configured to let all message packets through until a denial of service attack is detected, in which case VPN guard portion **3609** would allow only client packet streams conforming to a keyed hopping sequence, such as that of the present invention.

[0343]Server proxy portion **3610** also operates at the kernel layer within website **3608** and catches incoming message packets from client computer **3604** at the VPN level. At step **3705**, server proxy portion **3610** authenticates the message packets at the kernel level within host computer **3604** using the destination IP address, UDP ports and discriminator fields. The authenticated message packets are then forwarded to the authenticated message packets to web server portion **3611** as normal TCP web transactions.

[0344]At step **3705**, web server portion **3611** responds to message packets received from client computer **3604** in accordance with the particular nature of the message packets by generating reply message packets. For example, when a client computer requests a webpage, web server portion **3611** generates message packets corresponding to the requested webpage. At step **3706**, the reply message packets pass through server proxy portion **3610**, which inserts data into the payload portion of the message packets that are used for forming the virtual private connection between host computer **3608** and client computer **3604** over computer network **3602**. Preferably, the data for forming the virtual private connection is contains field-hopping data, such as described above in connection with VPNs. Server proxy portion **3610** operates at the kernel layer within host computer **3608** to insert the virtual private connection data into the payload portion of the reply message packets. Preferably, the modified message packets sent by host computer **3608** to client computer **3604** conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol.

[0345]At step **3707**, the modified packets are sent from host computer **3608** over computer network **3602** and pass through firewall **3603**. Once through firewall **3603**, the modified packets are directed to client computer **3604** over LAN **3601** and are received at step **3708** by proxy application **3607** at the application layer within client computer **3604**. Proxy application **3607** operates to rapidly evaluate the modified message packets for determining whether the received packets should be accepted or dropped. If the virtual private connection data inserted into the received information packets conforms to expected virtual private connection data, then the received packets are accepted. Otherwise, the received packets are dropped.

[0346]While the present invention has been described in connection with the illustrated embodiments, it will be appreciated and understood that modifications may be made without departing from the true spirit and scope of the invention.

ENGLISH-CLAIMS:
Return to Top of Patent

What is claimed is:

1. A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name, the method comprising:

- -

  receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device; and
- -

  sending a message over a secure communication link from the first device to the second device.

2. A method of using a first device to communicate with a second device having a secure name, the method comprising:

- -

  from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;
- -

  at the first device, receiving a message containing the network address associated with the secure name of the second device; and
- -

  from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

3. The method according to claim 2 , wherein the secure name of the second device is a secure domain name.

4. The method according to claim 2 , wherein the secure name indicates security.

5. The method according to claim 2 , wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted

form.

6. The method according to claim 5 , further including decrypting the message.

7. The method according to claim 2 , wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed.

8. The method according to claim 2 , wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device.

9. The method according to claim 2 , further including automatically initiating the secure communication link after it is enabled.

10. The method according to claim 2 , wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.

11. The method according to claim 2 , wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.

12. The method according to claim 2 , wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols.

13. The method according to claim 2 , wherein the receiving and sending of messages through the secure communication link includes multiple sessions.

14. The method according to claim 2 , further including supporting a plurality of services over the secure communication link.

15. The method according to claim 14 , wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

16. The method according to claim 15 , wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.

17. The method according to claim 15 , wherein the plurality of services comprises audio, video or a combination thereof.

18. The method according to claim 2 , wherein the secure communication link is an authenticated link.

19. The method according to claim 2 , wherein the first device is a computer, and the steps are performed on the computer.

20. The method according to claim 2 , wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.

21. The method according to claim 2 , further including providing an unsecured name associated with the device.

22. The method according to claim 2 , wherein the secure name is registered prior to the step of sending a message to a secure name service.

23. The method according to claim 2 , wherein the secure name of the second device is a secure, non-standard domain name.

24. A method of using a first device to securely communicate with a second device over a

communication network, the method comprising:

- -

  at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;
- -

  receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and
- -

  sending a message securely from the first device to the second device.

25. The method according to claim 24 , wherein requesting and obtaining registration of a secure name for the first device comprises using the first device to obtain a registration of the secure name for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.

26. A method of using a first device to communicate with a second device over a communication network, the method comprising:

- -

  from the first device requesting and obtaining registration of an unsecured name associated with the first device;
- -

  from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device;
- -

  receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and
- -

  from the first device sending a message securely from the first device to the second device.

27. The method according to claim 26 ,

- -

  wherein requesting and obtaining registration of an unsecured name associated with the first device comprises using the first device to obtain a registration of the unsecured name associated with the first device, and
- -

  wherein requesting and obtaining registration of a secure name associated with the first device comprises using the first device to obtain a registration of the secure name associated with the first device.

28. A non-transitory machine-readable medium comprising instructions for:

- -

  sending a message to a secure name service, the message requesting a network address associated with a secure name of a device;

- -

  receiving a message containing the network address associated with the secure name of the device; and

- -

  sending a message to the network address associated with the secure name of the device using a secure communication link.

29. A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name, the method comprising:

- -

  receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and

- -

  sending a message securely from the first device to the second device.

LOAD-DATE: March 5, 2012

Source: **Legal > Area of Law - By Topic > Patent Law > Find Patents > Utility, Design and Plant Patents** i
Terms: **patno=8051181** (Suggest Terms for My Search)
View: Full
Date/Time: Friday, April 6, 2012 - 5:24 PM EDT

1. Challenge to Social Networking Patent Among the Reexamination Requests Filed Week of March 26, 2012, Patent Law Practice Center, April 4, 2012 Wednesday 5:23 AM EST, , 1328 words
2. Virnetx Holding up Over 10% on Patent Denial., Benzinga.com, December 19, 2011, 275289577, 162 words
3. Certain Devices With Secure Communication Capabilities, Components Thereof, and Products Containing the Same; Institution of Investigation, U.S. International Trade Commission Documents and Publications, December 7, 2011, REGULATORY DOCUMENTS, 882 words
4. U.S. International Trade Commission Issues Notice Regarding Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing the Same, Targeted News Service, December 1, 2011 Thursday 5:32 AM EST, , 943 words, Targeted News Service, WASHINGTON
5. UNITED STATES : VirnetX claims Apple Inc, Tendersinfo News, November 9, 2011 Wednesday 6:30 AM EST, , 130 words
6. VirnetX Files Complaint Against Apple with International Trade Commission., Benzinga.com, November 7, 2011, 271847633, 120 words
7. VirnetX Files Complaint Against Apple with International Trade Commission., Benzinga.com, November 7, 2011, 271847667, 929 words
8. Briefing.com: Hourly In Play (R) - 23:00 ET, Briefing.com, November 7, 2011 Monday 11:00 PM EST, , 21879 words
9. Briefing.com: Hourly In Play (R) - 22:00 ET, Briefing.com, November 7, 2011 Monday 10:00 PM EST, ; 21879 words
10. Briefing.com: Hourly In Play (R) - 21:00 ET, Briefing.com, November 7, 2011 Monday 9:00 PM EST, , 21879 words

Source: **News & Business > Combined Sources > News, All (English, Full Text)** ⓘ
Terms: **8051181 or 8,051,181** (Suggest Terms for My Search)
View: Cite
Date/Time: Friday, April 6, 2012 - 5:26 PM EDT

Switch Client | Preferences | Help | Sign Out

My Lexis™ | Search | Get a Document | *Shepard's*® | More | History | Alerts

All | Legal | News & Business | Find A Source | Patent Law | Public Records | Add/Edit Subtabs

Legal > Area of Law - By Topic > Patent Law > Find Cases > Patent Cases from Federal Courts and Administrative Materials i

Search

View Tutorial | Help

Broaden this search with additional sources

☑ **Patent Cases from Federal Courts and Administrative Materials** i *(Source you selected)*

□ Chisum on Patents i

□ Patent Law Digest i

□ Patent Case Management Judicial Guide i

□ Intellectual Property Counseling and Litigation i

□ Court of Appeals for the Federal Circuit Practice & Procedure i

View all sources

Select Search Type and Enter Search Terms

Terms & Connectors

Natural Language

Easy Search™

8051181 or 8,051,181

Suggest terms for my search

Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment

Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

● No Date Restrictions ○ From To Date formats...

Search Connectors

and	and	w/p	in same paragraph
or	or	w/seg	in same segment
w/N	within N words	w/s	in same sentence
pre/N	precedes by N words	and not	and not

More Connectors & Commands...

How Do I...?

Combine sources?
Restrict by date?
Restrict by document segment?
Use wildcards as placeholders for one or more characters in a search term?

View Tutorials

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us

No Documents Found

No documents were found for your search terms

"8051181 or 8,051,181 "

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Search Using Natural Language" to run your search as Natural Language search.

- OR -

Click "Edit Search" to return to the search form and modify your search.

Suggestions:

- Check for spelling errors.
- Remove some search terms.
- Use more common search terms, such as those listed in "Suggested Words and Concepts."
- Use a less restrictive date range.
- Use "OR" in between terms to search for one term or the other.

| **Save this Search as an Alert** || **Search Using Natural Language** || **Edit Search** |

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us

Switch Client | Preferences | Help | Sign Out

My Lexis™ | Search | Get a Document | *Shepard's*® | More   History   Alerts

All   Legal   News & Business   Find A Source | Patent Law | Public Records   Add/Edit Subtabs

Legal > Area of Law - By Topic > Patent Law > Search News > Patent, Trademark & Copyright Periodicals, Combined i

Search   View Tutorial | Help

Select Search Type and Enter Search Terms

Terms & Connectors   8051181 or 8,051,181   Suggest terms for my search

Natural Language

Easy Search™   Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment   **Add**

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

● No Date Restrictions   ○ From ____ To ____   Date formats...

Search Connectors

and	and	w/p	in same paragraph
or	or	w/seg	in same segment
w/N	within N words	w/s	in same sentence
pre/N	precedes by N words	and not	and not

More Connectors & Commands...

How Do I...?
Combine sources?
Restrict by date?
Restrict by document segment?
Use wildcards as placeholders for one or more characters in a search term?

View Tutorials

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us

No Documents Found

No documents were found for your search terms
"8051181 or 8,051,181 "

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Search Using Natural Language" to run your search as Natural Language search.

- OR -

Click "Edit Search" to return to the search form and modify your search.

Suggestions:

- Check for spelling errors.
- Remove some search terms.
- Use more common search terms, such as those listed in "Suggested Words and Concepts."
- Use a less restrictive date range.
- Use "OR" in between terms to search for one term or the other.

| **Save this Search as an Alert** || **Search Using Natural Language** || **Edit Search** |

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us

Patent Assignment Abstract of Title

Total Assignments: 3

Application #: 11679416 **Filing Dt:** 02/27/2007 **Patent #:** 8051181 **Issue Dt:** 11/01/2011

PCT #: NONE **Publication #:** US20080005792 **Pub Dt:** 01/03/2008

Inventors: Victor Larson, Robert Dunham Short III, Edmund Colby Munger, Michael Williamson

Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Assignment: 1

Reel/Frame: 019463 / 0762 **Received:** 06/21/2007 **Recorded:** 06/21/2007 **Mailed:** 06/22/2007 **Pages:** 4

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: LARSON, VICTOR **Exec Dt:** 11/06/2003
SHORT, ROBERT DUNHAM, III **Exec Dt:** 10/27/2003
MUNGER, EDMUND COLBY **Exec Dt:** 11/05/2003
WILLIAMSON, MICHAEL **Exec Dt:** 11/05/2003

Assignee: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
10260 CAMPUS POINT DRIVE
SAN DIEGO, CALIFORNIA 92121

Correspondent: ATABAK R. ROYAEE
28 STATE STREET
MCDERMOTT WILL & EMERY, LLP
BOSTON, MA 02109

Assignment: 2

Reel/Frame: 019464 / 0133 **Received:** 06/21/2007 **Recorded:** 06/21/2007 **Mailed:** 06/22/2007 **Pages:** 6

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION **Exec Dt:** 12/21/2006

Assignee: VIRNETX, INC.
5615 SCOTTS VALLEY DRIVE, SUITE 110
SCOTTS VALLEY, CALIFORNIA 95066

Correspondent: ATABAK R. ROYAEE
28 STATE STREET
MCDERMOTT WILL & EMERY, LLP
BOSTON, MA 02109

Assignment: 3

Reel/Frame: 027558 / 0291 **Received:** 01/19/2012 **Recorded:** 01/19/2012 **Mailed:** 01/20/2012 **Pages:** 3

Conveyance: CHANGE OF ADDRESS OF ASSIGNEE

Assignor: VIRNETX INC. **Exec Dt:** 01/19/2012

Assignee: VIRNETX INC.
P.O. BOX 439
ZEPHYR COVE, NEVADA 89448

Correspondent: MCDERMOTT WILL & EMERY LLP
600 13TH STREET NW
WASHINGTON, DC 20005

Search Results as of: 04/09/2012 11:12 AM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.2.1
Web interface last modified: Jan 26, 2012

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,949	03/28/2012	8051181

CONFIRMATION NO. 4522

ASSIGNMENT NOTICE

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

OC000000053626087

Date Mailed: 04/10/2012

NOTICE OF ASSIGNMENT OF *INTER PARTES* REEXAMINATION REQUEST

The above-identified request for *inter partes* reexamination has been assigned to Art Unit 3992. All future correspondence in this proceeding should be identified by the control number listed above and directed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or, if none is of record, to all owners of record. (See 37 CFR 1.33(c).) If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s)

(MPEP 2222). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned with the request to withdraw pursuant to Section 1.36.

cc: Third Party Requester
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

/sdstevenson/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,949	03/28/2012	8051181

CONFIRMATION NO. 4522

REEXAM ASSIGNMENT NOTICE

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

OC000000053626086

Date Mailed: 04/10/2012

NOTICE OF *INTER PARTES* REEXAMINATION REQUEST FILING DATE

Requester is hereby notified that the filing date of the request for *inter partes* reexamination is 03/28/2012, the date that the filing requirements of 37 CFR § 1.915 were received.

A decision on the request for *inter partes* reexamination will be mailed within three months from the filing date of the request for *inter partes* reexamination. (See 37 CFR 1.923.)

A copy of this Notice is being sent to the person identified by the requestor as the patent owner. Further patent owner correspondence will be with the latest attorney or agent of record in the patent file. (See 37 CFR 1.33.) Any paper filed should include a reference to the present request for *inter partes* reexamination (by Reexamination Control Number) and should be addressed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

cc: Patent Owner
23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

/sdstevenson/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

23630 7590 06/04/2012

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	PAPER NUMBER
3992	
MAIL DATE	DELIVERY MODE
06/04/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

ORDER GRANTING/DENYING REQUEST FOR* INTER PARTES *REEXAMINATION	**Control No.** 95/001,949	**Patent Under Reexamination** 8051181
	Examiner DENNIS BONSHOCK	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

The request for *inter partes* reexamination has been considered. Identification of the claims, the references relied on, and the rationale supporting the determination are attached.

Attachment(s): □ PTO-892 ☒ PTO/SB/08 □Other: _____

1. ☒ The request for *inter partes* reexamination is GRANTED.

☒ An Office action is attached with this order.

□ An Office action will follow in due course.

2. □ The request for *inter partes* reexamination is DENIED.

This decision is not appealable. 35 U.S.C. 312(c). Requester may seek review of a denial by petition to the Director of the USPTO within ONE MONTH from the mailing date hereof. 37 CFR 1.927. EXTENSIONS OF TIME ONLY UNDER 37 CFR 1.183. In due course, a refund under 37 CFR 1.26(c) will be made to requester.

All correspondence relating to this *inter partes* reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Order.

DECISION

The present Request for *inter partes* reexamination, filed 3-28-2012, establishes a reasonable likelihood that the requestor will prevail with respect to claims 1-29 of United States Patent Number 8,051,181 (Larson et al.).

References Cited in the Request

A total of 12 references have been asserted in the request as providing teachings relevant to the claims of the Larson patent. These references are listed on page 2 of the request. The proposed references are as follows:

A. **Beser** – U.S. Patent No. 6,496,867

B. **Mattaway** – U.S. Patent No. 6,131,121

C. **Lendenmann** – "Understanding OSF DCE 1.1 for AIX and OS/2"

D. **Provino** – U.S. Patent No. 6,557,037

E. **RFC 2131** – "Dynamic Host Configuration Protocol"

F. **Johnson** – U.S. Patent No. 6,499,108

G. **H.323** – "Packet-based multimedia communications systems"

H. **H.225** – "Call signaling protocols and media stream packetization for packet-based multimedia communication systems"

I. **H.235** – "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals"

J. **H.245** – "Infrastructure of audiovisual services"

K. **RFC 1034** – "Domain Names – Concepts and Facilities"

L. **RFC 2401**– "Security Architecture for the Internet Protocol" (as included in Parent Application)

Identification of Every Claim for Which Reexamination is Requested

The 12 references cited above are discussed in various combinations regarding claims 1-29 of the Larson patent. Pages 1-318 of the Request detail out explanations that seek to establish a reasonable likelihood that the requestor will prevail with respect to at least one of the patent claims in light of the combinations of the 12 references cited above. The explanations in the Request are addressed below.

Prosecution History

Though the original Examiner provided no reasons for allowance the Reasons for Allowance, dated 7-18-2011, was in response to Remarks filed by the applicant, dated 6-7-2011. In these Remarks, the applicant (now patent owner) argued that the features of "a secure communication link", "a secure name service", and "a secure name" were lacking from the prior art applied.

> *First: Aventail fails to disclose "a secure name service" and a 'secure name." Aventail discloses conventional domain name services and domain names. Indeed, in reexamination of the "180 Patent, the Patent Office found that Aventail discloses a conventional "DNS server and the creation of a secure tunnel to a secure remote site Reexamination Control No. 95/001,270, Action Closing Prosecution, June 16, 2010, Exhibit B, at paragraph 6-7. Aventail does not disclose a non-conventional system, ld. In*

> *contrast to Aventail, paragraphs [0318] --- [0320] of the present application distinguish the claimed invention from conventional systems. See, generally, Nieh Dec. at paragraph 10-13. Aventail also does not teach the claimed secure communication link. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network° Id. at paragraph 25. Avemail discloses establishing point-to-point SOCKS connections between a client computer and a SOCKS server, ld. The SOCKS server then relays data received to the intended target. Id. Aventail does not disclose a secure communication link, where data can be addressed to a target, regardless of the location of the target. See, general/3." id, paragraph 24-27.*
>
> *Second: Aventail Connect's fundamental operation is incompatible with users transmitting data that are sensitive to network information. Id. at paragraph 28*
>
> *Third: Aventail has not been shown to disclose a secure communication link because computers connected according to Aventail do not communicate directly with each other. Id. at paragraph 29.*

The ' 180 patent, which is a parent to the ' 181 patent, has been the subject of two prior reexaminations. It should be noted that during the first reexamination, Control No. 95/001,270, the Patent Owner distinguished the methods and systems claimed in the ' 181 patent by asserting that the claim terms "secure domain name" and "secure domain name service" had particular meanings that were not equivalent to conventional meanings associated with the terms domain name and domain name service. In particular, the ' 180 patentee stated:

> *The ' 180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a convention[all domain name server using a secure domain name will result in a return message indicating that the URL is unknown ('180 patent at 51:25-35) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name ('180 patent at 51:25-35).*

The '181 patent owner also has taken a position as to what the terms "secure domain name" and "secure domain name service" as used in the ' 181 patent claims may encompass. For example, the ' 181 patent owner stated:

> *[T]he Applicant submits that a "secure name" is a name associated with a network address associated of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device. The claimed "secure name" includes, but is not limited to, a secure domain name. For example, a "secure name" can be a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number.*

Thus, the file history of the '181 patent and the reexamination records of the related '180 patent contain representations made by the ' 181 patent owner that the Patent Office may properly consider in evaluating the broadest reasonable construction that can be given to the claims of the ' 181 patent.

Reasonable Likelihood to Prevail (RLP) on the Issue of Patentability

The claims for which reexamination is requested will be utilized to show whether the above-cited references, taken together with the explanation provided by requester, are found to establish, or not to establish, that there is a reasonable likelihood that the requester will prevail with respect to at least one of the patent claims.

Issue 1 **– Beser (anticipation)**

The proposed rejection of claims 1-29, as set forth on pages 23-65 of the Request and pages 1-8 of the Appendix: '181 Patent Claim Charts is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Beser teaches Unsecure Names / IP addresses of end devices being associated with unique identifiers (such as phone numbers, email addresses, domain name), where this association is made at a third party network device, that provides routing between end devices via the retained list of association. Beser further teaches Secure Names / private IP address of end devices that are packetized so as to translate a packet between end devices where source / destination addresses are of intermediary linking devices (first 14, second 16, trusted third party 30), not the Originating 24 and Terminating 26 devices, who's address is hidden within the packet. (see column 11, line 25 through column 12, line 19, column 10, lines 36-41, and figure 1)

Claims 1-12, 14, 15, and 17-29

Beser appears to teach each and every limitation of claims 1-12, 14, 15, and 17-29 (see pages 23-40, 41-42, and 43-65 of the Request and pages 1-8 of the Exhibit C1 '181 Patent Claim Charts, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 1-12, 14, 15, and 17-29.

Claim 13

Beser does not teach "wherein the receiving and sending of messages through the secure communication link includes multiple sessions" of claim 13. There is no mention in the cited portions of the reference of "multiple sessions". The Request appears to imply that such a limitation would be inherently required by Baser in view of the teachings of column 4, lines 43-54, however the cited passage does not provide adequate direction that such a teaching would be inherent. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 13, since it is deemed that Baser does not teach the missing limitations as noted with regards to claim 13.

Claim 16

Beser does not teach "wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof" of claim 16. Though the cited portion (Beser at 4:43-54) provides support for telephony devices, there is no mention in the cited portions of the reference of video conferencing, e-mail, a word processing program, so as to make up the combination. Additionally, though the reference states

"Telephony devices include...personal computers running facsimile or audio applications", it appears that it is either a facsimile application or an audio application, precluding the reading of the claim as a plurality of different telephony applications. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 16, since it is deemed that Baser does not teach the missing limitations as noted with regards to claim 16.

Therefore, it is found that the consideration of Beser **establishes** that there is a reasonable likelihood that the requester will prevail with respect to **claims 1-12, 14, 15, and 17-29**.

Conversely, it is found that the consideration of Beser **does not establish** that there is a reasonable likelihood that the requester will prevail with respect to **claims 13 and 16**.

***Issue 2* – Beser and RFC2401 (obviousness)**

The proposed rejection of claim 18, as set forth on pages 65-67 of the Request, is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

The Request appears to imply that the limitations of claim 18 would be obvious in view of the teachings of Beser and RFC2401, unfortunately the Request fails to provide any evidence or for that matter any explanation of how or why the teachings of the two references would or could be combined. Instead, the Request appears to avoid addressing the issue of what specific teachings are being combined, how the teachings are combined, or why such a combination would be proper with respect to the combination of Beser and RFC2401, rather the Request provides teachings from both references that the Requestor believes reads on the claim, while not providing specific of what claim element either reference lacks. Additionally, the Requester argued in the preceding issue (Issue 1) that Larson taught each and every limitation of claim 18, leaving it even more unclear why the combination with RFC2401 is now being proposed or for which teaching RFC2401 supplements. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 18, since it is deemed that the combination of Beser and RFC2401 does not teach the missing limitations as noted with regards to claim 18.

Therefore, it is found that the consideration of the combination of Beser and RFC2401 **does not establish** that there is a reasonable likelihood that the requester will prevail with respect to claim 18.

Issue 3 – **Mattaway (anticipation)**

The proposed rejection of claims 1-2, 5-9, 12-17, 19-22, and 24-29, as set forth on pages 68-94 of the Request and pages 1-8 of Exhibit C2 '181 Patent Claim Charts and is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Mattaway teaches a connection server 26 that maintains a database 34 of callee email addresses and associated IP addresses, so that when a request is made for a connection via a caller, the caller can be connected to the callee via the association stored at the server. (see column 7, lines 20-36)

Claims 1, 2, 6-9, 12-17, 19-21, and 24-29

Mattaway appears to teach each and every limitation of claims 1, 2, 6-9, 12-17, 19-21, and 24-29 (see pages 68-94 of the Request and pages 1-8 of Exhibit C2 '181 Patent Claim Charts, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 1, 2, 6-9, 12-17, 19-21, and 24-29.

Claim 5

Mattaway does not teach "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form" of claim 5. Though the cited portion (Mattaway at 35:32-34) provides support for telephone communication being encrypted, there is no mention in the cited portions of the reference to encrypting the message containing the network address associated with the secure name of the second device. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 5, since it is deemed that Mattaway does not teach the missing limitations as noted with regards to claim 5.

Claim 22

Mattaway does not teach "wherein the secure name is registered prior to the step of sending a message to a secure name service" of claim 22. There is no cited portions of the reference provided. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 22, since it is deemed that Mattaway does not teach the missing limitations as noted with regards to claim 22.

Therefore, it is found that the consideration of Mattaway **establishes** that there is a reasonable likelihood that the requester will prevail with respect to **claims 1, 2, 6-9, 12, 14-17, 19-21, and 24-29.**

Conversely, it is found that the consideration of Mattaway **does not establish** that there is a reasonable likelihood that the requester will prevail with respect to **claims 5, 13, and 22.**

***Issue 4* – Mattaway in view of Beser (obviousness)**

The proposed rejection of claims 3-4, 10-11, 18, and 23, as set forth on pages 94-98 of the Request is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Mattaway in view of Beser appear to teach each and every limitation of claims 3-4, 10-11, 18, and 23 (see pages 94-98 of the Request, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 3-4, 10-11, 18, and 23.

Therefore, it is found that the consideration of Mattaway in view of Beser **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claims 3-4, 10-11, 18, and 23.

Issue 5 **– Mattaway in view of RFC2401 (obviousness)**

The proposed rejection of claims 10 and 11, as set forth on pages 98-100 of the Request is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Mattaway in view of RFC2401 appears to teach each and every limitation of claims 10 and 11 (see pages 98-100 of the Request, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 10 and 11.

Therefore, it is found that the consideration of Mattaway in view of RFC2401 **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claim 10 and 11.

Issue 6 **– Lendenmann (anticipation)**

The proposed rejection of claims 1-9, 12-15, and 18-29, as set forth on pages 101-159 of the Request and on pages 1-7 of Exhibit C3 '181 Patent Claim Charts, is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Lendenmann teaches a Cell Directory Service (CDS) that stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource. (see page 21) Where the client can utilize the namespace maintained by the CDS for the location of a server that handles the interface that the client is interested in (see page 182). Lendenmann further teaches the DCE Naming Service that allows user to identify, by name, resources such as servers, files, disks, or print queues, and gain access to them without needing to know where they are located in a network. (see page 22) Lendenmann further allows for cell name aliasing so as to have a primary name, and one or more alias names that is recognized by DCE services (see page 24). This dual name scheme in Lendenamann provides two naming schemes:

- CCITT X.500 [secure]
- Intemet Domain Name Service (DNS) [not secure]

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Altematively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." An example of an X.500 name is: [Cell name] [CDS name]. (see page 23)

Lendenmann appears to teach each and every limitation of claims 1-9, 12-15, and 18-29 (see pages 101-159 of the Request and pages 1-7 of Exhibit C3 '181 Patent Claim Charts, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 1-9, 12-15, and 18-29.

Therefore, it is found that the consideration of Lendenmann **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claims 1-9, 12-15, and 18-29.

***Issue 7*– Lendenmann in view of Beser (obviousness)**

The proposed rejection of claims 10-11 and 16-17, as set forth on pages 160-164 of the Request is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Claims 10, 11, and 17

Lendenmann in view of Beser appear to teach each and every limitation of claims 10, 11, and 17 (see pages 160-164 of Request, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 10, 11, and 17.

Therefore, it is found that the consideration of Lendenmann in view of Beser **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claim 10, 11, and 17.

Claim 16

Lendenmann in view of Beser does not teach "wherein the plurality of application programs comprises video conferencing, email, a word processing program, telephony or a combination thereof" of claim 16. There is no mention in the cited portions of the reference of multiple application programs from the recited list. Additionally, though the Beser reference states "Telephony devices include...personal computers running facsimile or audio applications", it appears that it is either a facsimile application or an audio application, precluding the reading of the claim as a plurality of different telephony applications. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 16, since it is deemed that Beser does not teach the missing limitations as noted with regards to claims 16.

Therefore, it is found that the consideration of Lendenmann in view of Beser **does not establish** that there is a reasonable likelihood that the requester will prevail with respect to claim 16.

Issue 8 **– Lendenmann in view of RFC 2401 (obviousness)**

The proposed rejection of claims 10 and 11, as set forth on pages 164-166 of the Request, is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Lendenmann in view of RFC 2401 appear to teach each and every limitation of claims 10 and 11 (see pages 164-166 of the Request, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 10 and 11.

Therefore, it is found that the consideration of Lendenmann in view of RFC 2401 **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claim 10 and 11.

Issue 9 **– Provino (anticipation)**

The proposed rejection of claims 1-23 and 28-29, as set forth on pages 167-188 of the Request and on pages 1-8 of Exhibit C4 '181 Patent Claim Charts and is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Provino teaches use of an unsecured name where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43). Provino further teaches use of a secure name where the device my only establish a secure communication link upon receipt of the secure name (the integer Internet address which is registered on the VPN name server (see column 9, line 56 through column 10, line 7, column 9, lines 17-27, and column 13, liens 26-67), Provino teaches that "*the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30.*" (see column 13, lines 54-67) Here the initiating device has the email address / domain name and requests the actual IP address.

Claims 1-15, 18-23, 28, and 29

Provino appears to teach each and every limitation of claims 1-15, 18-23, 28, and 29 (see pages 167-188 of the Request and on pages 1-8 of Exhibit C4 '181 Patent Claim Charts, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 1-15, 18-23, 28, and 29.

Therefore, it is found that the consideration of Provino **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claims 1-15, 18-23, 28, and 29.

Claim 16

Provino does not teach "wherein the plurality of application programs comprises video conferencing, email, a word processing program, telephony or a combination thereof" of claim 16. There is no mention in the cited portions of the reference of the plurality of the applications comprising elements from the listed set. The Request appears to imply that such a limitation would be inherent in view of the teachings of Provino, unfortunately the Request fails to provide any evidence or for that matter any explanation in support of this implication. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 16.

Claim 17

Provino does not teach "wherein the plurality of services comprises audio, video or a combination thereof" of claim 17. There is no mention in the cited portions of the reference of the services including audio or video. The Request appears to imply that such a limitation would be inherent in view of the teachings of Provino, unfortunately the Request fails to provide any evidence or for that matter any explanation in support of this implication. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claim 17.

Therefore, it is found that the consideration of Provion **does not establish** that there is a reasonable likelihood that the requester will prevail with respect to claims 16 and 17.

Issue 10 – **Provino in view of H.323 (obviousness)**

The proposed rejection of claims 24-26, as set forth on pages 188-203 of the Request is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Provino in view of H.323 appears to teach each and every limitation of claims 24-26 (see pages 188-203 of the Request, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 24-26.

Therefore, it is found that the consideration of Provino in view of H.323 **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claims 24-26.

Issue 11 – **H.323 (anticipation)**

The proposed rejection of claims 1-29, as set forth on pages 204-268 of the Request and on pages 1-8 of Exhibit C5 '181 Patent Claim Charts and is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

H.323 teaches secure names (name with associated access token) and unsecure names (alias names or gateway address) (see pages 33-35 and 38). H.323. further teaches endpoints registering with a gatekeeper so as to register a secure name and then be associated with the unsecured name of the gatekeeper thereby being accessed via an alias (see page 35).

H.323 appears to teach each and every limitation of claims 1-29 (see pages 204-268 of the Request and on pages 1-8 of Exhibit C5 '181 Patent Claim Charts, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 1-29.

Therefore, it is found that the consideration of H.323 **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claim 1-29.

***Issue 12* – H.323 in conjunction with H.224, H.235, and H.245 (obviousness)**

The proposed rejection of claims 1-29, as set forth on page 269 of the Request is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

The Request appears to imply that claims 1-29 are obvious under H.323 in conjunction with H.224, H.235, and H.245, unfortunately the Request fails to provide any evidence or for that matter any explanation in support of this implication. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claims 1-29

Therefore, it is found that the consideration of H.323 in conjunction with H.224, H.235, and H.245 **does not establish** that there is a reasonable likelihood that the requester will prevail with respect to claims 1-29.

***Issue 13* – Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401 (obviousness)**

The proposed rejection of claims 1-16 and 18-29, as set forth on pages 270-318 of the Request and on pages 1-9 of Exhibit C6 '181 Patent Claim Charts, is relied upon to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the Larson patent.

Johnson teaches a secure name being registered by the secure mail server with the secure name server. (see column 10, lines 36-52)

Johnson discloses that the a first device securely communicated with the secure name server in order to request a network address that is associated with the secure name--which is associated with the network address---of the second device, i.e., the secure mail server. At 11:21-37, Johnson explains: *Process to Get an Address from a Secure Name Server FIG. 7 of the drawings outlines the process by which an unknown address, such as* ***the dynamic address of a secure mail server, is obtained from a secure name server.*** *The process starts by selecting the target secure name server machine by its fixed address/name as shown in block 150. The user then provides the secure name server with its logon protocol combination as shown at block 152. If the user logon combination is verified then a session is established with a secure name server as shown at block 154. ...if the session has been correctly established as shown at block 156, then the user will be allowed to request the address for the named machine at the client site as shown at block 158.*

Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401 appear to teach each and every limitation of claims 1-16 and 18-29 (see pages 270-318 of the Request and on pages 1-9 of Exhibit C6 '181 Patent Claim Charts, hereby incorporated by reference). Hence, it is found that the requester has shown a reasonable likelihood of success with respect to claims 1-16 and 18-29.

Therefore, it is found that the consideration of Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401 **establishes** that there is a reasonable likelihood that the requester will prevail with respect to claims 1-16 and 18-29.

Summary

Claims 1-29 will be reexamined.

Conclusion

Extensions of time under 37 CFR 1.136(a) will not be permitted in inter partes reexamination proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to the patent owner in a reexamination proceeding. Additionally, 35 U.S.C. 314(c) requires that inter partes reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.937). Patent owner extensions of time in inter partes reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner's response is set by statute. 35 U.S.C. 314(b)(3).

The Patent Owner is reminded of the continuing responsibility under 37 CFR 1.985(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the US Patent 8,051,181 throughout the course of this reexamination proceeding. The Third Party Requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding through the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

All correspondence relating to this inter partes reexamination proceeding should be directed as follows:

By U.S. Postal Service Mail to:

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:

(571) 273-9900
Central Reexamination Unit

By hand to:

Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/Dennis G. Bonshock/
Primary Examiner, Art Unit 3992

ALEXANDER J. KOSOWSKI
Supervisory Patent Reexamination Specialist
CRU -- Art Unit 3992

/Adam L Basehoar/
Primary Examiner, Art Unit 3992

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

23630 7590 06/04/2012
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	PAPER NUMBER
3992	
MAIL DATE	DELIVERY MODE
06/04/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

Date:

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

OFFICE ACTION IN* INTER PARTES *REEXAMINATION	**Control No.** 95/001,949	**Patent Under Reexamination** 8051181
	Examiner DENNIS BONSHOCK	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on _____
Third Party(ies) on 28 March, 2012

RESPONSE TIMES ARE SET TO EXPIRE AS FOLLOWS:

For Patent Owner's Response:
2 MONTH(S) from the mailing date of this action. 37 CFR 1.945. EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.956.
For Third Party Requester's Comments on the Patent Owner Response:
30 DAYS from the date of service of any patent owner's response. 37 CFR 1.947. NO EXTENSIONS OF TIME ARE PERMITTED. 35 U.S.C. 314(b)(2).

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

This action is not an Action Closing Prosecution under 37 CFR 1.949, nor is it a Right of Appeal Notice under 37 CFR 1.953.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1.☐ Notice of References Cited by Examiner, PTO-892
2.☒ Information Disclosure Citation, PTO/SB/08
3.☐ _____

PART II. SUMMARY OF ACTION:

1a. ☒ Claims 1-29 are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled.
3. ☐ Claims _____ are confirmed. [Unamended patent claims]
4. ☐ Claims _____ are patentable. [Amended or new claims]
5. ☒ Claims 1-29 are rejected.
6. ☐ Claims _____ are objected to.
7. ☐ The drawings filed on _____ ☐ are acceptable ☐ are not acceptable.
8. ☐ The drawing correction request filed on _____ is: ☐ approved. ☐ disapproved.
9. ☐ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has: ☐ been received. ☐ not been received. ☐ been filed in Application/Control No 95001949.
10. ☐ Other _____

DETAILED ACTION

This Office action addresses claims 1-29 of United States Patent Number 8,051,181 (Larson et al.) for which it has been determined in the Order Granting Inter Partes Reexamination (hereafter the "Order") that a substantial new question of patentability was raised in the Request for *inter partes* reexamination filed on 3-28-2012 (hereafter the "Request").

Information Disclosure Statement

MPEP 2656 states in pertinent part:

Where patents, publications, and other such items of information are submitted by a party (Patent Owner or Requester) in compliance with the requirements of the rules, the requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information. The initials of the examiner placed adjacent to the citations on the form PTO/SB/08A and 08B or its equivalent, without an indication to the contrary in the record, do not signify that the information has been considered by the examiner any further than to the extent noted above.

In concert with MPEP 2656, the references submitted in the IDS have been considered only to the extent that the content and relevance of the references have been explained.

Rejections Proposed by the Requester

A total of 12 references have been asserted in the Request as providing teachings relevant to the claims of the Larson patent. In view of the Order, 10 of the proposed issues have established a reasonable likelihood that the Requester will prevail. The following proposed rejections are the main issues to be discussed below:

Issue 1: Claims 1-12 in view of Beser

Issue 3: Claims 1, 2, 6-9, 12, 14-17, 19-21, and 24-29 in view of Mattaway

Issue 4: Claims 3-4, 10-11, 18, and 23 in view of Mattaway in view of Beser

Issue 5: Claims 10 and 11 in view of Mattaway in view of RFC2401

Issue 6: Claims 1-9, 12-15, and 18-29 in view of Lendenmann

Issue 7: Claims 10, 11, and 17 in view of Lendenmann in view of Beser

Issue 8: Claims 10 and 11 in view of Lendenmann in view of RFC2401

Issue 9: Claims 1-15, 18-23, 28, and 29 in view of Provino

Issue 10: Claims 24-26 in view of Provino in view of H.323

Issue 11: Claims 1-29 in view of H.323

Issue 13: Claims 1-16 and 18-29 in view of Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401

Claim Rejection Paragraphs

Claim Rejections - 35 USC § 102

The following are quotations from the MPEP regarding the types of rejections to be utilized below:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Issue 1

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-12, 14, 15, and 17-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-12, 14, 15, and 17-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Beser (see pages 23-40, 41-42, and 43-65 of the Request and pages 1-8 of the Exhibit C1 '181 Patent Claim Charts, incorporated by reference).

Issue 3

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1, 2, 6-9, 12-17, 19-21, and 24-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1, 2, 6-9, 12, 14-17, 19-21, and 24-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Mattaway (see pages 68-94 of the Request and pages 1-8 of Exhibit C2 '181 Patent Claim Charts, incorporated by reference).

Claim 13 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 76 of the Request and pages 4 of Exhibit C2 '181 Patent Claim Charts, incorporated by reference), the Requester lacked a citation to go alone with the quote they cited from the Mattaway reference, which is being herein supplemented by the Examiner.

Mattaway discloses that each call, i.e., session, "may be assigned a successive session number in sequence, which may be used by the respective processing unit to associate the call with one of the SLIP/PPP lines, to associate a <ConnectOK> response signal from a <ConnectRequest> signal, and to allow for multiplexing and demultiplexing of inbound and outbound conversations on conference lines .... " (see column 6, lines 24-36)

Issue 4

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 3-4, 10-11, 18, and 23 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 3-4, 10-11, 18, and 23 are rejected under 35 U.S.C. 103(e) as being obvious over Mattaway in view of Beser (see pages 94-98 of the Request, incorporated by reference).

Issue 5

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10 and 11 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10 and 11 rejected under 35 U.S.C. 103(e) as being obvious over Mattaway in view of RFC2401 (see pages 98-100 in the Request, incorporated by reference).

Issue 6

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-9, 12-15, and 18-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-9, 12-15, and 18-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Lendenmann (see pages 101-159 of the Request and pages 1-7 of Exhibit C3 '181 Patent Claim Charts, incorporated by reference).

Issue 7

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10, 11, and 17 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10, 11, and 17 are rejected under 35 U.S.C. 103(e) as being obvious over Lendenmann in view of Beser (see pages 160-164 of Request, incorporated by reference).

Issue 8

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10 and 11 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10 and 11 are rejected under 35 U.S.C. 103(e) as being obvious over Lendenmann in view of RFC 2401 (see pages 164-166 of the Request, incorporated by reference).

Issue 9

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-15, 18-23, 28, and 29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-12, 18-23, 28, and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Provino (see pages 167-203 of the Request and pages 1-8 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference).

Claim 13 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 3 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 1, lines 1-24:

> *The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection there between, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the*

> *network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The* ***external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.***

This paragraph provides support for a plurality of communications being provided during the period when the secure connection channel is enabled.

Claim 14 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 4 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 5, lines 28-35:

> *If the received message packets contain information, such as* ***Web pages or the like****, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit.* ***In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.***

This paragraph provides support for a plurality of different services being provided.

Claim 15 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 4 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 1, lines 1-24:

> *The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection there between, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The* ***external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.***

Provino teaches in column 5, lines 28-35:

> *If the received message packets contain information, such as* ***Web pages or the like****, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit.* ***In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.***

These paragraphs provide support for multiple sessions and a plurality of application programs.

Issue 10

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 24-26 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 24-26 are rejected under 35 U.S.C. 103(e) as being obvious over Provino in view of H.323 (see pages 188-203 of the Request, incorporated by reference).

Issue 11

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-9 and 12-29 are rejected under 35 U.S.C. 102(b) as being obvious over H.323 (see pages 204-268 of the Request and on pages 1-8 of Exhibit C5 '181 Patent Claim Charts, incorporated by reference).

Claims 10 and 11 are adopted with clarification, as additionally rejected under 35 U.S.C. 102(b) (see pages 230-231 of the Request and on page 3 of Exhibit C5 '181 Patent Claim Charts, incorporated by reference)., the Requester lacked an appropriate supporting citation to go alone with the anticipation claim made with respect to the H.323 reference, which is being herein supplemented by the Examiner.

H.323 teaches on page 59:

> ***In order to conserve resources, synchronize call signaling and control, and reduce call setup time, it may be desirable to convey H.245 messages within the Q.931 call signaling channel instead of establishing a separate H.245 channel. This process, known as "encapsulation" or "tunneling" of H.245 messages****, is accomplished by utilizing the h245Control element of h323_uu_pdu on the call signaling channel, copying an encoded H.245 message as an octet string. When tunneling is active, one or more H.245 messages can be encapsulated in any Q.931 message. If tunneling is being utilized and there is no need for transmission of a Q.931 message at the time an H.245 message must be transmitted, then a FACILITY message shall be sent with h323-message-body set to empty.*

This paragraph provides support for tunneling.

Issue 13

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-16 and 18-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-16 and 18-29 are rejected under 35 U.S.C. 103(e) as being obvious over Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401 (see pages 270-318 of the Request and on pages 1-9 of Exhibit C6 '181 Patent Claim Charts in the Request, incorporated by reference).

Conclusion

Extensions of time under 37 CFR 1.136(a) will not be permitted in inter partes reexamination proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to the patent owner in a reexamination proceeding. Additionally, 35 U.S.C. 314(c) requires that inter partes reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.937). Patent owner extensions of time in inter partes reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner's response is set by statute. 35 U.S.C. 314(b)(3).

The Patent Owner is reminded of the continuing responsibility under 37 CFR 1.985(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the US Patent 8,051,181 throughout the course of this reexamination proceeding. The Third Party Requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding through the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

All correspondence relating to this inter partes reexamination proceeding should be directed as follows:

By U.S. Postal Service Mail to:

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:

(571) 273-9900
Central Reexamination Unit

By hand to:

Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/Dennis G. Bonshock/
Primary Examiner, Art Unit 3992

/Adam L Basehoar/
Primary Examiner, Art Unit 3992

Substitute for form PTO/SB/42 **INFORMATION DISCLOSURE STATEMENT BY REQUESTOR**		**Complete if Known**	
		Docket Number	41484-80200
		Application/Control No.	
		Confirmation No.	
		Examiner	
		Group Art Unit	
		Patent No. under Reexamination	8,051,181
		Inventor	Larson et al.
		Issue Date	November 1, 2011
Sheet 1	of 1		

U.S. PATENT DOCUMENTS

Examiner Initials	Cite #	DOCUMENT NUMBER	CODE	NAME	ISSUE DATE (mm/dd/yyyy)	CLASS	SUB CLASS	Filing Date if Appropriate
	X2	6131121	A	Mattaway et al	10/10/2000	709	227	
	X1	6496867	B1	Beser et al.	12/17/2002	709	245	
	X6	6499108	B1	Johnson, R.	12/24/2002	713	201	
	X4	6557037	B1	Provino, J.	04/29/2003	709	227	

OTHER DOCUMENTS

Examiner Initials	Cite #	Include Author, Title, Date, Pertinent Pages, etc.
	X3	Lendenmann, R. et al., "Understanding OSF DCE 1.1 for AIX and OS/2," IBM Corporation International Technical Support Organization (October 1995); pp. 1-274.
	X5	Droms, R. RFC 2131, "Dynamic Host Configuration Protocol" (November 1987); pp. 1-39.
	X7	ITU-T Recommendation H.323, "Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services. Packet-based multimedia communications systems," International Telecommunications Union (February 1998); pp. 1-128.
	X8	ITU-T Recommendation H.225.0, "Infrastructure of audiovisual services – Transmission multiplexing and synchronization. Call signalling protocols and media stream packetization for packet-based multimedia communication systems," International Telecommunication Union (February 1998); pp. 1-155.
	X9	ITU-T Recommendation H.235, "Infrastructure of audiovisual services – Systems aspects. Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," International Telecommunication Union (February 1998); pp. 1-39.
	X10	ITU-T Recommendation H.245, "Infrastructure of audiovisual services – Communication procedures. Control protocol for multimedia communication," International Telecommunication Union (February 1998); pp. 1-280.
	X11	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities" (November 1987); pp. 1-47.

Examiner Signature	/Dennis Bonshock/	Date Considered	05/30/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

Notice of References Cited	Application/Control No. 95/001,949	Applicant(s)/Patent Under Reexamination 8051181
	Examiner DENNIS BONSHOCK	Art Unit 3992 / Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Atkinson, R., RFC 2401, "Security Architecture for the Internet Protocol" (November 1998); pp. 1-66
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No. 95001949	Applicant(s)/Patent Under Reexamination 8051181
	Examiner DENNIS BONSHOCK	Art Unit 3992

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
Reviewed all prosecution history	5-22-12	dgb

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Reexamination	**Application/Control No.** 95001949	**Applicant(s)/Patent Under Reexamination** 8051181
	Certificate Date	**Certificate Number**

Requester Correspondence Address: □ **Patent Owner** ☒ **Third Party**

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

LITIGATION REVIEW ☒	DGB (examiner initials)	05/23/2012 (date)

Case Name	Director Initials
VirnetX Inc. v. Cisco Systems, Inc., Apple, Inc., et al., Civ	

COPENDING OFFICE PROCEEDINGS

TYPE OF PROCEEDING	**NUMBER**

Patent Owner Attorney Docket No. 077580-0160

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Victor Larson, et al.	)	
	)	
U.S. Patent No.: 8,051,181	)	
Filed: February 27, 2007	)	**Examiner:**
Issued*:* November 1, 2011	)	**DENNIS G. BONSHOCK**
	)	
For: METHOD FOR ESTABLISHING	)	**Group Art Unit: 3992**
SECURE COMMUNICATION LINK	)	
BETWEEN COMPUTERS OF	)	
VIRTUAL PRIVATE NETWORK	)	
	)	
Reexamination Proceeding	)	
Control No.: 95/001,949	)	
Filed: March 28, 2012	)	

PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.956 TO REPLY TO OFFICE ACTION IN REEXAMINATION

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

VirnetX Inc. ("VirnetX"), the owner of the above-referenced patent ("the '181 patent"), hereby petitions the Director for a one-month extension of time for responding to the Office Action mailed June 4, 2012 ("Office Action") in the above-identified reexamination proceeding. A response to the Office Action is currently due on or before August 6, 2012[1]. A one-month extension would extend the deadline to and including September 4, 2012.

For reasons stated more fully below, the extension of time requested is necessary to fully and completely address the rejections set forth in the Office Action which is itself

[1] August 4, 2012 is a Saturday.

twenty-three (23) pages long and partially incorporates by reference **319** **<u>single-space</u>** **pages** of the Request for Reexamination filed March 28, 2012, <u>plus</u> an additional **49** **pages of claim charts**. The size and complexity of the issues raised by the Office Action is exacerbated by (1) the continuing need to investigate whether the seven cited non-patent literature references[2] have been appropriately asserted as prior art, and (2) working with a technical expert to generate an appropriate § 1.132 declaration.

Further straining the ability of the Patent Owner to respond to the outstanding rejections are (3) multiple concurrent reexamination proceedings of patents related to the above-referenced patent, as described below, which have caused a significant drain on the availability of the Patent Owner's resources, and (4) the concurrent litigation involving the above-referenced patent, as well as three other litigation proceedings involving related patents, which also has caused a significant drain on the Patent Owner's resources, especially the inventors who are believed necessary to prepare a proper response to the Office Action. In light of these factors, as more fully explained below, the Patent Owner respectfully requests a one-month extension of time to and including September 4, 2012 to respond to the outstanding Office Action.

Pursuant to 37 C.F.R. § 1.956, this petition for an extension of time is being filed well before the due date for the response, and sets forth sufficient reasons for the extension, as detailed below.

I. Complexity of the Office Action and Work With an Expert

Preparing a response to the Office Action will involve substantial analysis requiring significant time and resources. The Office Action is twenty-three (23) pages in length. It partially incorporates by reference <u>319 single-spaced pages</u> of the Request for Reexamination filed March 28, 2012 ("Request"), plus the six claim charts incorporated

[2] Req. Ex. X3 ("Understanding OSF DCE 1.1 for AIX and OS/2"), Req. Ex. X5 ("Dynamic Host Configuration Protocol"), Req. Ex. X7 ("Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services. Packet-based multimedia communications systems"), Req. Ex. X8 ("Infrastructure of audio visual services – Transmission multiplexing and synchronization. Call signalling protocols and media stream packetization for packet-based multimedia communication systems"), Req. Ex. X9 ("Infrastructure of audiovisual services – Systems aspects. Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals"), Req. Ex. X10 ("Infrastructure of audiovisual services – Communication procedures. Control protocol for multimedia communication"), and Req. Ex. X11 ("Domain Names – Concepts and Facilities").

by that request adding another 49 pages for a total of **391 pages**. In addition, the Office Action incorporates **1,092 pages** from eleven (11) different references alleged to be prior art, including 130 pages of patent publications, and 962 pages of non-patent literature references, all of which must be analyzed in depth before making a timely response. The references which must be considered are cited—either alone and/or in various combinations—as supporting **thirteen (13) different grounds of rejection (Issues)**.

While the Patent Owner has begun analysis of the Office Action, the 319 pages of the Request incorporated by it, and the eleven (11) references on which it relies, the complexity of those references and their application to the claims in thirteen (13) different grounds of rejection require a more in-depth analysis and comparison by personnel of the Patent Owner, including one or more of the inventors, whose availability within the two month period for response to the Office Action has been and will continue to be limited, as discussed below.

The complexity of the issues presented by the Office Action is exacerbated by its reliance on some references that have not been shown to be either a patent or a printed publication, as is required to support a rejection in reexamination. In particular, it appears that there is insufficient support to establish that at least the non-patent references cited by the Office Action were printed publications prior to the priority date of the '181 patent. For example, the Request asserts that "Understanding OSF DCE 1.1 for AIX and OS/2" was "distributed publicly without restriction no later than October 1995" without any stated support. The Request asserts that "Dynamic Host Configuration Protocol" was "publicly distributed no later than March of 1997" without any stated support. The Request asserts that "Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services. Packet-based multimedia communications systems" was "publicly distributed no later than February of 1998" without any stated support. The Request asserts that "Infrastructure of audio visual services – Transmission multiplexing and synchronization. Call signalling protocols and media stream packetization for packet-based multimedia communication systems" was "publicly distributed no later than February of 1998" without any stated support. The Request asserts that "Infrastructure of audiovisual services – Systems aspects. Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals" was "publicly distributed no later than November of 1998" without any stated support. The Request asserts that "Infrastructure of audiovisual services – Communication procedures. Control protocol for multimedia communication" was "publicly distributed no later than February of 1998" without any stated support. The Request also asserts that "Domain Names – Concepts and Facilities" was "publicly distributed no later than November of 1987" without any stated support.

The Patent Owner continues to investigate whether these references have been appropriately asserted as prior art and will likely need to address those issues in a response to the Office Action. However, because rejections have been issued based on those references, they must now be addressed twice, once regarding whether they are proper prior art and once substantively in response to the rejections in the Office Action.

In addition, the Patent Owner is considering providing the Examiner with the views of an independent technical expert in a § 1.132 declaration. However, working with an expert can be very time consuming even under normal circumstances. With thirteen (13) grounds of rejection based on eleven (11) different references, the work and necessary time is expected to be much greater than normal. In addition, the Patent Owner must accommodate the work schedule and the availability of the expert to assist in a response.

III. Concurrent Reexamination Proceedings

The instant reexamination proceeding is not the only one thrust on the Patent Owner at this time. Rather, the Patent Owner is or will be concurrently handling several other pending reexamination proceedings, including the following being handled by the same below-signed counsel: (1) control no. 95/001,697 involving U.S. Patent No. 7,490,151 ("the '151 patent"), (2) control no. 95/001,788 involving U.S. Patent No. 7,418,504 ("the '504 patent"), (3) control no. 95/001,789 involving U.S. Patent No. 7,921,211 ("the '211 patent"), and (4) control no. 95/001,682 involving U.S. Patent No. 6,502,135 ("the '135 patent"). These proceedings are related to the instant proceeding in that the subject patents are related to one another and will demand substantial attention from VirnetX's counsel during the period for response to the outstanding Office Action. Additionally, while some of the issues are similar among these proceedings, preparing complete responses to any future office actions will require, by any standard, a very significant amount of time and effort. Declarations from a technical expert also may be used in these related proceedings, meaning that counsel for VirnetX will be coordinating with one or more technical experts to prepare multiple responses and declarations.

IV. Concurrent Litigation

Just at the time when the Patent Owner is in need of significant resources to respond to this Office Action and tend to the other reexamination proceedings mentioned above, many of those very resources are being taxed by the pending litigation proceedings involving the '181 patent, and three other pending litigation proceedings involving other related patents owned by the Patent Owner. The '181 patent is currently a subject of litigation in Case No. 6:11-cv-563 in the Eastern District of Texas captioned *VirnetX, Inc. v. Apple, Inc.*, a litigation in which the Requester itself is involved. The '181 patent is also currently a subject of International Trade Commission Investigation No. 337-TA-818, in which the Requester is involved. The resources and availability of various personnel of the Patent Owner are being drained by these proceedings. As a result, resources and personnel of the Patent Owner required to fully and accurately prepare a response to the Office Action are currently limited.

V. Conclusion

For the reasons stated above, the Patent Owner believes that a one-month extension is appropriate. A prompt decision granting this extension of time is respectfully requested to allow the Patent Owner a fair opportunity to respond to the present Office Action.

VirnetX is concurrently submitting payment of the requisite fees with the undersigned's request that the requisite fees be charged to this firm's Deposit Account 50-1133. Please charge any additional fees due and/or credit any excess fees paid in connection with the filing of this paper to Deposit Account 50-1133.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/ John A. Hankins /
John A. Hankins, Reg. No. 32,029
Toby H. Kusmer, P.C., Reg. No. 26,418
Kenneth C. Cheney, Reg. No. 61,841
McDermott Will & Emery LLP
Attorneys for the Patent Owner

Please recognize our Customer No. 23630 as our correspondence address.

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com
Date: June 25, 2012

Attorney Docket No. 077580-0160

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Victor Larson, et al.	)	
	)	
U.S. Patent No.: 8,051,181	)	
Filed: February 27, 2007	)	**Examiner:**
Issued: November 1, 2011	)	**DENNIS G. BONSHOCK**
	)	
For: METHOD FOR ESTABLISHING	)	**Group Art Unit: 3992**
SECURE COMMUNICATION LINK	)	
BETWEEN COMPUTERS OF	)	
VIRTUAL PRIVATE NETWORK	)	
	)	
Reexamination Proceeding	)	
Control No.: 95/001,949	)	
Filed: March 28, 2012	)	

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the **PATENT OWNER'S PETITION FOR EXTENSION OF TIME PURSUANT TO 37 C.F.R. § 1.956**, filed with United States Patent and Trademark Office on June 25, 2012, was served this June 25, 2012 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, Texas 75201

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/ John A. Hankins /
John A. Hankins, Reg. No. 32,029
Toby H. Kusmer, P.C., Reg. No. 26,418
Kenneth C. Cheney, Reg. No. 61,841
McDermott Will & Emery LLP
Attorneys for the Patent Owner
Please recognize our Customer No. 23630 as our correspondence address.

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com
Date: June 25, 2012

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	John A. Hankins/Kimila Carraway
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**200**

Electronic Acknowledgement Receipt

EFS ID:	13100167
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	23630
Filer:	John A. Hankins/Kimila Carraway
Filer Authorized By:	John A. Hankins
Attorney Docket Number:	41484-80200
Receipt Date:	25-JUN-2012
Filing Date:	28-MAR-2012
Time Stamp:	20:00:05
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$200
RAM confirmation Number	6817
Deposit Account	502624
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		077580-0160_Petition_Extension_Time_Office_Action_Reexamination.pdf	54629 a56dfe2e0e0efc58ec5377e46bde244b58eddacb	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Reexam Request for Extension of Time	1	6
Reexam Certificate of Service	7	7

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30594 4183b78ac19ee525c77fbc311eb58cdcd178e3c4	no	2

Warnings:

Information:

Total Files Size (in bytes):	85223

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

23630 7590 06/27/2012

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	

ART UNIT	PAPER NUMBER

DATE MAILED: 06/27/2012

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

Decision on Petition for Extension of Time in Reexamination	95/001,949

1. THIS IS A DECISION ON THE PETITION FILED: 25 June 2012.

2. THIS DECISION IS ISSUED PURSUANT TO:
   A. □ 37 CFR 1.550(c) – The time for taking any action by a patent owner in an *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   B. ☒ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS
   Patent owner requests that the period for responding to the Office action dated 04 June 2012 which sets a two (2) month period for filing a response to the Office action, be extended by one (1) month.

   A. ☒ Petition fee per 37 CFR §1.17(g)):
      i. □ Petition includes authorization to debit a deposit account.
      ii. □ Petition includes authorization to charge a credit card account.
      iii. □ Other: ______________.
   B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
   C. ☒ Petition was timely filed.
   D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
   A. ☒ Granted or □ Granted-in-part for one (1) month, because petitioner provided a factual accounting that established sufficient cause. (See 37 CFR 1.550(c) and 37 CFR 1.956).
   B. □ Other/comment: ______________.
   C. □ Dismissed because:
      i. □ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).
      ii. □ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
      iii. □ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
      iv. □ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
      v. □ The petition is moot.
      vi. □ Other/comment: see attachment.

5. CONCLUSION

   Telephone inquiries with regard to this decision should be directed to Mark Reinhart at 571-272-1611. In his absence, calls may be directed to Sudhanshu C Pathak at 571-272-5509 in the Central Reexamination Unit.

/Mark Reinhart/	SPRS, AU 3992 Central Reexamination Unit
[*Signature*]	(Title)

U.S. Patent and Trademark Office
PTO-2293 (Rev. 09-2010)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PETITION SEEKING WAIVER OF 37 C.F.R. § 1.943 FOR PATENT OWNER'S RESPONSE TO OFFICE ACTION OF JUNE 4, 2012

Pursuant to 37 C.F.R. § 1.183, Patent Owner VirnetX Inc., ("VirnetX") requests that the Director waive the requirement of 37 C.F.R. § 1.943(b) limiting Patent Owner's responses to 50 pages in length. Specifically, VirnetX requests that the Office accept its 78-page response to the June 4, 2012, Office Action ("Office Action").[1] VirnetX is submitting this petition concurrently with its response.

To the extent that entry and consideration of this petition requires suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. In addition, a petition fee of $400 is being submitted with this petition. If there is any other fee due in connection with the filing of this petition, please charge the fee to Deposit Account No. 502624.

Rule 1.943(b) states that "[r]esponses by the patent owner and written comments by the third party requester [cannot] exceed 50 pages in length, excluding . . . reference materials." 37 C.F.R. § 1.943(b). VirnetX seeks entry and consideration of this petition so that it can comprehensively address all the issues raised by the Examiner in the Office Action. Specifically, the Office Action adopted, in whole or in part, eleven grounds of rejections based on eleven different combinations of references proposed by the third-party requester, Apple Inc. ("Apple"). In doing so, the Office

[1] The listed page and word count excludes the pages and words that constitute the "amendments, appendices of claims, and reference materials" as the Office has interpreted that language of 37 C.F.R. § 1.943(b).

Action relied on and incorporated by reference corresponding portions of the 319 pages of Apple's request and 49 pages of accompanying claim charts. VirnetX seeks adequate opportunity to comprehensively address the issues raised in the Office Action.

VirnetX, therefore, requests that the Director waive the page-limit requirements of § 1.943(b) and permit VirnetX to submit an Office Action response containing 78 pages and two supporting declarations.

I. BACKGROUND

On March 28, 2012, Apple Inc. initiated an *inter partes* reexamination of all claims 1-29 of the '181 patent. In its request, Apple proposed thirteen rejections based on thirteen different combinations of references. The Office granted Apple's request for reexamination of all claims 1-29 of the '181 patent on June 4, 2012 and assigned it control no. 95/001,949 ("'1,949 proceeding"). (*See* 6/4/2012 Order Granting/Denying Request for *Inter Partes* Reexamination, "Order.") On June 4, 2012, the Office also issued an Office Action, adopting, in whole or in part, eleven of the thirteen rejections proposed by Apple in its request for reexamination. (*See* 6/4/2012 Office Action, "Office Action" or "OA".)

In adopting Apple's proposed rejections, the Office Action adopted and incorporated by reference the corresponding portions of the 319 pages of Apple's request and accompanying claim charts C1-C6. (*See* OA at 3-12.)

VirnetX's response to the Office Action is 78 pages long. In addition, VirnetX is submitting two declarations, one from Dr. Robert Dunham Short III (one of the inventors of the '181 patent) and another one from Angelos D. Keromytis, Ph.D. (an expert). The declaration of Dr. Short presents facts regarding secondary considerations and the declaration of Dr. Keromytis discusses how one of ordinary skill in the art would have understood the references cited in the Office Action.

II. ARGUMENT

Under 37 C.F.R. § 1.943(b), "[r]esponses by the patent owner and written comments by the third party requester [cannot] exceed 50 pages in length, excluding . . . reference materials." Because of the numerous issues raised in the Office Action and the incorporation by reference of 319 pages of Apple's request and 49 pages of accompanying claim charts, VirnetX requests that the Office accept its response that has 78 pages. VirnetX has made every effort to pare down its response, but submits that limiting its response to 50 pages would severely compromise its ability to fully address the issues raised in the Office Action.

VirnetX's response seeks to comprehensively address the rejections adopted by the Examiner. In adopting eleven of the grounds of rejection proposed by Apple in whole or in part, the

Examiner incorporated by reference corresponding portions of the 319 pages of Apple's request and 49 pages of accompanying claim charts. VirnetX's response to the Office Action seeks to address all the issues raised by the Examiner. Thus, given all of the issues, justice requires that the Office allow VirnetX to file its response, which contains 78 pages.

As noted above, with its response, VirnetX is also submitting two declarations, one by Dr. Short, one of the inventors, and another by Dr. Keromytis, an expert. The declaration of Dr. Short presents facts regarding secondary considerations and the declaration of Dr. Keromytis discusses how one of ordinary skill in the art would have understood the references cited in the Office Action. Given their content, VirnetX does not believe that either declaration counts towards the page limit. Nevertheless, should the Office decide to include portions of either declaration in the page count for the response, VirnetX requests that the Office waive the requirements of Rule 1.943(b) and permit it to submit these declarations with its response. Indeed, even if the Office were to count the declarations towards the page limit, the total number of pages representing the response and the declarations would still be substantially less than the 319 pages of Apple's request and 49 pages of accompanying claim charts relied upon and incorporated by reference in the Office Action.

III. CONCLUSION

For the foregoing reasons, VirnetX requests that the Office grant this petition and accept its Office Action response, which contains 78 pages and exceeds the page count limitations imposed by 37 C.F.R. § 1.943(b).

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/John A. Hankins/
John A. Hankins, Reg. No. 32,029
Toby H. Kusmer, P.C., Reg. No. 26,418
Kenneth C. Cheney, Reg. No. 61,841
Ricky K. Chun, Reg. No. 63,371
Michael G. Dreznes, Reg. No, 59,965
McDermott Will & Emery LLP
Attorneys for Patent Owner

4 Park Plaza, Suite 1700
Irvine, California 92614-2559
Telephone: (949) 851-0633
Facsimile: (949) 851-9348
Date: September 4, 2012

**Please recognize our Customer No. 23630
as our correspondence address.**

APPENDIX - LIST OF EXHIBITS

EXHIBIT	DESCRIPTION
A-1	Verdict Form from *VirnetX, Inc. v. Microsoft Corp.*, No. 6:07-CV-80 (E.D. Tex.).
A-2	Defendants' Responsive Claim Construction Brief from *VirnetX, Inc. v. Cisco Systems, Inc.*, No. 6:10-CV-00417 (E.D. Tex.).
A-9	Defendants' Motion for Reconsideration of the Construction of the Term "Secure Communication Link" from *VirnetX, Inc. v. Cisco Systems, Inc.*, No. 6:10-CV-00417 (E.D. Tex.).
B-1	Excerpt from Department of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999.
B-2	Collection of Reports and Presentations on DARPA Projects.
B-3	Maryann Lawlor, *Transient Partnerships Stretch Security Policy Management*, SIGNAL Magazine (Sept. 2001), http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes.
B-4	Joel Snyder, *Living in Your Own Private Idaho*, Network World (January 26, 1998), http://www.networkworld.com/intranet/0126review.html.
B-5	Tim Greene, *CEOs Chew the VPN Fat*, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch.

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	John A. Hankins/Brian Vo
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition fee- 37 CFR 1.17(f) (Group I)	1462	1	400	400
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**400**

Electronic Acknowledgement Receipt

EFS ID:	13656250
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	23630
Filer:	John A. Hankins/Brian Vo
Filer Authorized By:	John A. Hankins
Attorney Docket Number:	41484-80200
Receipt Date:	04-SEP-2012
Filing Date:	28-MAR-2012
Time Stamp:	20:21:54
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$400
RAM confirmation Number	7782
Deposit Account	502624
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		TransandCOC.pdf	83520 942318ab8553071739aa4e327f82c5de570d8285	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**		**End**
	Trans Letter filing of a response in a reexam		1		2
	Reexam Certificate of Service		3		4
Warnings:					
Information:					
2	Response after non-final action-owner timely	Reexamresponse.pdf	946965 ec54ac75d4dd530db55a2770f769e92f3d41e3c1	no	83
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Short_Declaration.pdf	492952 5a5dccb21e771a700afe317ace1183a9cb14a722	no	5
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Keromytis_Declaration.pdf	1005722 66e9bae29e510240a8837328f1d288a58258b546	no	72
Warnings:					
Information:					
5	Receipt of Petition in a Reexam	Petition.pdf	89078 1865dad4c134e0606099254ffb1720dfa3302bbc	no	3
Warnings:					
Information:					
6	Miscellaneous Incoming Letter	Appendix_listofexhibits.pdf	76605 bfd22ec2b0e63a16638c1784b83c0abca940fcd2	no	1
Warnings:					
Information:					
7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitA1_pdf.pdf	929836 fd4e53090145ce7448820aaca8d852d037cb5c3e	no	3
Warnings:					
Information:					

8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitA2_pdf.pdf	288512 e8353cc35e9c0fe008ae276fff7ef54ddc17e994	no	38
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EXHIBITA9_pdf.pdf	95469 91ca5ab36e41ffafe84f8c0e8334c82882b33167	no	8
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitB1_pdf.pdf	11018464 276d498063c59448a949a5196c9a7eaba09fef6a	no	23
Warnings:					
Information:					
11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitB2_.pdf	16431789 bf555f36c46b75d615609510c7b32c76c45e7f7c	no	95
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitB3.pdf	252387 8055d209d920e88a44c8371da6b75a5ad343691a	no	5
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitB4_pdf.pdf	3138836 6901ef5e0a5a559714000f6f7f0f8f17bf80f6c1	no	5
Warnings:					
Information:					
14	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	ExhibitB5_pdf.pdf	2852157 b1e7b65c41cdea876d8df8565509832f5f0d7018	no	6
Warnings:					
Information:					
15	Fee Worksheet (SB06)	fee-info.pdf	30367 0171281a9106a347945d347de583dedc46f0021b	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	37732659	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

-

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE	)	Confirmation No. 4522
COMMUNICATION LINK BETWEEN	)	
COMPUTERS OF A VIRTUAL PRIVATE	)	
NETWORK	)	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

TRANSMITTAL LETTER

Enclosed please find the following:

1. Patent Owner's Response to Office Action (78 pages);
2. Declaration of Angelos D. Keromytis, Ph.D. (38 pages) with appended *curriculum vitae*;
3. Declaration of Dr. Robert Dunham Short III (5 pages);
4. Appendix - List of Exhibits (1 page);
5. Exhibits Listed on Appendix;
6. Petition Seeking Waiver of 37 C.F.R. § 1.943 for Patent Owner's Response to Office Action of June 4, 2012 (3 pages);
7. Petition Fee of $400; and
8. Certificate of Service (2 pages).

Please grant any extension of time and charge any additional fees to Deposit Account No. 502624.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/John A. Hankins/
John A. Hankins, Reg. No. 32,029
Toby H. Kusmer, P.C., Reg. No. 26,418
Kenneth C. Cheney, Reg. No. 61,841
Ricky K. Chun, Reg. No. 63,371
Michael G. Dreznes, Reg. No, 59,965
McDermott Will & Emery LLP
Attorneys for Patent Owner

4 Park Plaza, Suite 1700
Irvine, California 92614-2559
Telephone: (949) 851-0633
Facsimile: (949) 851-9348
Date: September 4, 2012

Please recognize our Customer No. 23630 as our correspondence address.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor Larson et al.) Control No.: 95/001,949
)
U. S. Patent No. 8,051,181) Group Art Unit: 3992
)
Issued: November 1, 2011) Examiner: Dennis G. Bonshock
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 4522
COMMUNICATION LINK BETWEEN)
COMPUTERS OF A VIRTUAL PRIVATE)
NETWORK)

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the Patent Owner certifies that copies of the following documents:

1. Transmittal Letter (2 pages);
2. Patent Owner's Response to Office Action (78 pages);
3. Declaration of Angelos D. Keromytis, Ph.D. (38 pages) with appended *curriculum vitae*;
4. Declaration of Dr. Robert Dunham Short III (5 pages);
5. Appendix - List of Exhibits (1 page);
6. Exhibits Listed on Appendix;
7. Petition Seeking Waiver of 37 C.F.R. § 1.943 for Patent Owner's Response to Office Action of June 4, 2012 (3 pages); and
8. Certificate of Service (2 pages)

were served by first-class mail on September 4, 2012 on counsel for the third-party Requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/John A. Hankins/
John A. Hankins, Reg. No. 32,029
Toby H. Kusmer, P.C., Reg. No. 26,418
Kenneth C. Cheney, Reg. No. 61,841
Ricky K. Chun, Reg. No. 63,371
Michael G. Dreznes, Reg. No, 59,965
McDermott Will & Emery LLP
Attorneys for Patent Owner

4 Park Plaza, Suite 1700
Irvine, California 92614-2559
Telephone: (949) 851-0633
Facsimile: (949) 851-9348
Date: September 4, 2012

Please recognize our Customer No. 23630 as our correspondence address.

PATENT
Customer No. 23,630
Attorney Docket No. 077580-0160

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U. S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S RESPONSE TO OFFICE ACTION OF JUNE 4, 2012

Table of Contents

I. Introduction

VirnetX Inc. ("VirnetX"), the owner of U.S. Patent No. 8,051,181 ("the '181 patent"), provides the following remarks in response to the Office Action ("OA") and Order granting reexamination ("Order") mailed June 4, 2012, in the above-identified reexamination proceeding. The U.S. Patent and Trademark Office ("USPTO" or "Office") issued the Office Action and Order in response to a Request for Reexamination ("Request") filed by Apple, Inc. ("Apple" or "Requester") on March 28, 2012.

The patent at issue in this reexamination (the '181 patent) is part of a family of patents ("Munger patent family") that stems from U.S. provisional application nos. 60/106,261 ("the '261 application"), filed on October 30, 1998, and 60/137,704 ("the '704 application"), filed on June 7, 1999. The '181 patent is a continuation of U.S. Patent 7,188,180, which is a divisional of U.S. application no. 09/558,209 ("the '209 application") filed April 26, 2000 (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent 6,502,135, "the '135 patent"). The '135 patent is a continuation-in-part of U.S. application no. 09/429,643 (now U.S. Patent 7,010,604, "the '604 patent"), which claims priority to the '261 and '704 applications.

The Office recently denied a request for reexamination of U.S. Patent 7,188,180, from which the '181 patent is a continuation. That request for reexamination raised many of the same references that are being raised in this reexamination. (Order in Control No. 95/001,792.) Other patents in the Munger family have also been subject to reexamination and district court actions. For instance, U.S. Patent 6,839,759, a continuation of the '209 application, and two other patents from the family were asserted in an action against Microsoft Corporation in the Eastern District of Texas. The jury found the asserted claims willfully infringed and not invalid, and awarded VirnetX over one hundred million dollars in damages. (Ex. A-1 at 2.) Microsoft had sought reexamination of two of the patents, but all claims were confirmed during those proceedings. (*See* Control Nos. 95/001,269 and 95/001,270.)

Given that the validity of the patents in the Munger patent family has now been tested multiple times, and for other reasons set forth below, including that the asserted references do not disclose or suggest the combination of features recited in the claims, VirnetX requests reconsideration and withdrawal of all the rejections in the Office Action and confirmation of the patentability of all of the claims of the '181 patent.

This Response is supported by a Declaration of Dr. Angelos D. Keromytis, Ph.D. ("Keromytis Decl.") and by a Declaration of Dr. Robert Dunham Short III ("Short Decl."), Ph.D.

II. Background

A. Overview of the ’181 Patent

The ’181 patent discloses several embodiments relating to establishing secure communication links (*e.g.*, a link supporting encrypted communications) between devices connected over a network. (Keromytis Decl. ¶ 15.) The subject technology provides a “secure name” and, in some embodiments, an “unsecure name,” associated with a remote device. (*Id.*) In some embodiments, the “secure name” may be represented by a hyperlink or desktop icon, and allows a user to enable the secure communication link with just a “single click” or other minimal input to the device. (’181 patent 50:23-30, 56-61.)

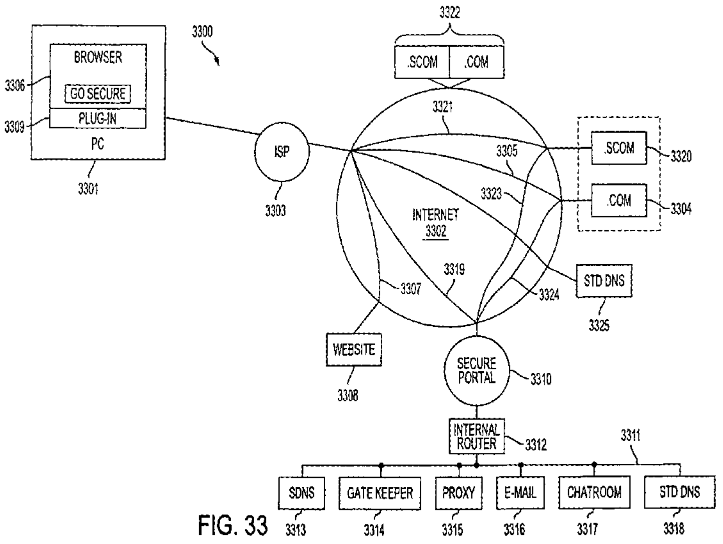


FIG. 33

In one embodiment, depicted in Fig. 33 of the ’181 patent, reproduced above, computer 3301 may communicate conventionally with another computer 3304 over a non-secure communication link 3305 through a network 3302. A web page provided by computer 3304 to computer 3301 may contain a “Go Secure” hyperlink or icon for enabling a secure communication mode of communication between computer 3301 and computer 3304 over network 3302. (’181 patent 50:54-61.) By selecting the displayed hyperlink or icon, the user enables a secure communication mode without having to enter user identification information, passwords, or encryption keys. (’181 patent 49:66-50:3.) Accordingly, in one example, a software module 3309 located on computer 3301 may begin a process that establishes a secure communication link between computer 3301 and computer 3304. (’181 patent 50:7-12.) The user may also enable the secure communication mode in other ways, such as, for example, by entering into the computer a command related to the "secure name" (*e.g.*, "go secure"). ('181 patent 49:39-40.)

When a secure communication mode has been initiated, software module 3309 may query a secure name service (3313) for a secure network address of computer 3304. ('181 patent 50:19-25.) The secure name service resolves secure names and facilitates establishing a secure communication link based on a secure name. (Keromytis Decl. ¶ 17.) In this respect, the secure name service cross-references secure names with corresponding network addresses for establishing secure communications with computer 3304. ('181 patent 50:60-67.) The secure name service returns a network address for computer 3304, ('181 patent 51:26-29), and computer 3301 uses the network address and other provided resources to communicate securely with computer 3304, ('181 patent 51:44-46).

The claims of the '181 patent are directed to some of these embodiments. Claims 1, 2, 24, 26, 28, and 29 are independent claims. Claims 3-23 depend directly or indirectly from claim 2, claim 25 depends from claim 24, and claim 27 depends from claim 26. As explained below, none of the references relied upon by the Office, either individually or in combination, discloses or suggests the combination of features recited in these claims.

B. Applicable Legal Standards for Anticipation

Anticipation of a claim requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations *arranged or combined in the same way* as recited in the claim, it . . . cannot anticipate under 35 U.S.C. § 102." *Net MoneyIn, Inc. v. Verisign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) (emphasis added). "The requirement that the prior art elements themselves be 'arranged as in the claim' means that claims cannot be 'treated . . . as mere catalogs of separate parts, in disregard of the part-to-part relationships set forth in the claims and that give the claims their meaning.'" *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010) (quoting *Lindemann Maschinenfabrik GmbH v. Am. Hoist & Derrick Co.*, 730 F.2d 1452, 1459 (Fed. Cir. 1984)).

C. Applicable Legal Standards for Obviousness

Obviousness is a question of law based on underlying factual inquiries, as set forth by *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). These factors include, among other things, ascertaining the differences between the claimed invention and the prior art. M.P.E.P. § 2141(II). "The question of obviousness must be resolved on the basis of these factual determinations," *id.*, which are determined "at the time the invention was made," *id.* at § 2143.02(III). Additionally, "[o]bjective evidence relevant to the issue of obviousness must be evaluated by Office personnel." M.P.E.P. § 2141(II).

"In determining the differences between the prior art and the claims, the question under 35 U.S.C. [§] 103 is not whether the differences *themselves* would have been obvious, but whether the claimed invention *as a whole* would have been obvious." M.P.E.P. § 2141.02(I). Consequently, "all of the claim limitations must be taught or suggested by the prior art applied and [ ] all words in a claim must be considered in judging the patentability of that claim against the prior art." *Ex Parte Karl Burgess*, Appeal 2008-2820, 2009 WL 291172 (B.P.A.I. 2009), at *3 (citing *In re Royka*, 490 F.2d 981, 984-85 (CCPA 1974), and *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970)). A rejection based on obviousness "cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 126 S. Ct. 1727, 1741 (2007) (citing *In re Kahn*, 441 F.3d at 988). The references relied upon for a rejection based on obviousness must also be enabling. M.P.E.P. § 2145.

III. The Rejections Should Be Withdrawn

The Office rejects claims 1-29 of the '181 patent as anticipated or obvious in view of several references. As explained below, however, the rejections are based on references that have not been properly established as being publically available before the effective filing date of the '181 patent and do not disclose or suggest the combination of features recited in the claims.

A. Certain References Have Not Been Shown to Be Prior Art

The Office and Requester rely on the following eight references to support the various rejections of the claims without evidencing that these references are in fact prior art:

1. Lendenmann, "Understanding OSF DCE 1.1 for AIX and OS/2" ("*Lendenmann*") (Req. Ex. X3);
2. Droms, R., RFC 2131, "Dynamic Host Configuration Protocol" ("*RFC 2131*") (Req. Ex. X5);
3. ITU-T H.323, "Packet-based multimedia communications systems" ("*H.323*") (Req. Ex. X7);
4. ITU-T H.225.0, "Call signalling protocols and media stream packetization for packet-based multimedia communication systems" ("*H.225.0*") (Req. Ex. X8);

5. ITU-T H.235, "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals" ("*H.235*") (Req. Ex. X9);
6. ITU-T H.245, "Infrastructure of audiovisual services – Communication procedures" ("*H.245*") (Req. Ex. X10);
7. Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities" ("*RFC 1034*") (Req. Ex. X11);
8. Kent, RFC 2401, "Security Architecture for IP" ("*RFC 2401*") (not submitted as exhibit to Req.).

Reexamination of an issued patent is limited to situations where a substantial new question of patentability has been shown "based on patents or printed publications." M.P.E.P. § 2247. The statutory phrase "printed publication" has been interpreted to mean that the alleged prior art reference must have been sufficiently accessible to the public interested in the art. *In re Cronyn*, 890 F.2d 1158, 1160 (Fed. Cir. 1989) (quoting *Constant v. Adv. Micro-Devices, Inc.*, 848 F.2d 1560, 1568 (Fed. Cir. 1988)). The party asserting the alleged prior art bears the burden of establishing a date of publication. *See In re Wyer*, 655 F.2d 221, 227 (C.C.P.A. 1981) ("the one who wishes to characterize the information, in whatever form it may be, as a 'printed publication' . . . '*should produce **sufficient proof*** of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents") (emphasis added); *see also* M.P.E.P. § 2128.

The Office and the Requester have not provided any evidence (such as by affidavit) that *Lendenmann*, *RFC 2131*, *H.323*, *H.225.0*, *H.235*, *H.245*, *RFC 1034*, or *RFC 2401* (together the "Asserted Publications"), were publicly available or that they are printed publications. *See In re Hall*, 781 F.2d 897 (Fed. Cir. 1986). The Asserted Publications contain no indication that they were published, or were even publicly available, before the effective filing date of the '181 patent. Copyright dates printed on the Asserted Publications do not establish that the Asserted Publications were indeed published on the copyright date listed. Unlike a publication date, a copyright date merely establishes "the date that the document was created or printed." *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003). A copyright date is "*insufficient as a matter of law* to establish that [a reference] was known or used by others" at that time. *Id.* (emphasis added); *cf. In re Wyer*, 655 F.2d at 227.

In addition, the Office merely adopts the Requester's bald assertion that *Lendenmann*, *RFC 2131*, *H.323*, *H.225.0*, *H.235*, *H.245*, and *RFC 1034* are "printed publications"[1] without making an initial determination as to whether these references have priority over the '181 patent. (*See generally* OA; Req. at 12-13.) Accordingly, the Requester's assertions are nothing more than attorney argument, and are not evidence that the Asserted Publications are "printed publications."

In view of the above, the Office and Requester have failed to demonstrate that any of the Asserted Publications is a "printed publication" sufficient to qualify as a prior art reference. Consequently, the rejections of the claims in view of these references (specifically, the rejections corresponding to Issues 1, 3, 5, 6, 8, and 10-13) should be withdrawn.

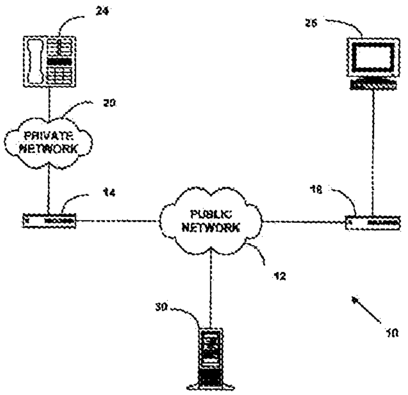
B. The Rejection of Claims 1-29 Under 35 U.S.C. § 102(e) Based on *Beser* Should Be Withdrawn (Issue 1)

The Office rejects claims 1-29 under § 102(e) based on U.S. Patent No. 6,496,867 to Beser et al. ("*Beser*"). (OA at 5.) For the reasons discussed below, this rejection should be withdrawn and the claims should be confirmed.

1. Overview of *Beser*

Beser discloses a system for initiating a tunneling association that hides the identity of the originating and terminating ends of the tunneling association from other users. (*Beser* Abstract.) With reference to Fig. 1, reproduced below, *Beser* describes that a request is received at a first network device 14, the request including a unique identifier for a terminating telephony device 26. (*Id.* at 10:2-6, 22-23.)

FIG. 1



The trusted-third-party network device 30 is informed of the request, and associates the unique identifier with a public IP address of a second network device 16. (*Id.* at 11:26-32.) Then,

[1] Requester did not provide any assertion or evidence whatsoever that *RFC 2401* was a printed publication prior to the filing date of the '181 patent.

private IP addresses for originating telephony device 24 and terminating telephony device 26 are negotiated and distributed to second network device 16 and first network device 14, respectively. (*Id.* at 11:59-12:54.) According to *Beser*, the tunneling association "hides the identity of the originating and terminating ends of the tunneling association from the other users of the public network." (*Id.* at 2:36-39.)

2. Independent Claim 1

a. *Beser* Fails to Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire[ ] to Securely Communicate with the First Device"

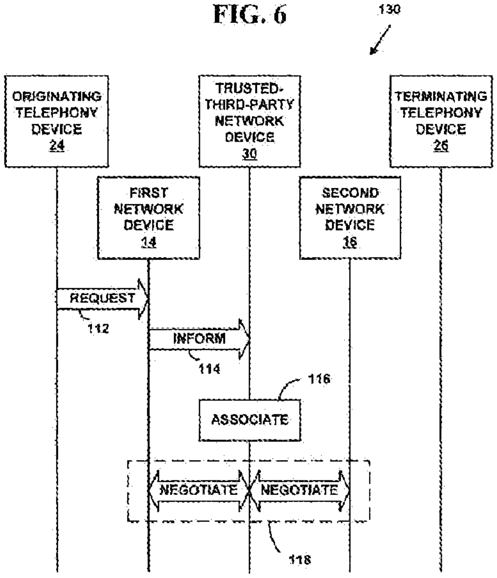
Claim 1 recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." *Beser* does not disclose this feature.

Requester never expressly identifies the elements of *Beser* that allegedly qualify as the claimed "message." (*See* Req. at 27-29.) Instead, Requester generally alleges that "*Beser* shows security measures can be utilized which result in receiving, at a network address corresponding to the secure device, a message from a second device of the desire to securely communicate. For example, tunneling—a method of communicating securely—is taught in *Beser*." (*Id.* at 28.) Requester then spends two paragraphs purporting to show that the tunneling connection is secure. (*Id.* at 28.) Nothing in these paragraphs discloses the claimed "message," and Requester does not assert that it does. (*Id.*) For example, in this part of the Request, Requester cites a brief example in *Beser* related to how packets can be tunneled. (Req. at 28, citing *Beser* 2:6-12.) That example, however, does not disclose "receiving . . . a message from a second device of the desired to securely communicate." Moreover, the cited example merely discloses encapsulating an IP packet in a payload field, and tunneling packets between end-points in an *already initiated* tunneling connection. (*See* Req. at 28, citing *Beser* 2:6-12.) Accordingly, the cited example cannot be used to evidence disclosure of the claimed "message."[2]

Next, Requester cites to Fig. 6 of *Beser*, reproduced below, and describes the function of trusted-third-party network device 30 after it allegedly receives a unique identifier from a querying device. (*Id.* at 29.)

[2] The cited example is also in the background section of *Beser*, and is *not* described as having anything to do with the other cited portions of *Beser*. Consequently the cited example cannot be used to support a rejection under § 102. *Net MoneyIN, Inc.*, 88 USPQ2d at 1758 (anticipation requires "all of the limitations arranged or combined in the same way as recited in the claim").

FIG. 6



But again, Requester does not point to what part of Fig. 6 allegedly discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." Indeed, none of the communications shown in Fig. 6 of *Beser* can be the claimed message. (Keromytis Decl. ¶ 22.) Specifically, "Request 112" cannot be the claimed message because this would require first network device 14 to be the claimed "first device" and originating telephony device 24 to be the claimed "second device." If this were true, then *Beser* does not disclose sending a message over a secure communication link from the first device to the second device because the alleged secure communication link (*i.e.*, *Beser*'s tunneling association, Req. at 29-31) is formed between originating telephony device 24 and terminating telephony device 26. (Keromytis Decl. ¶ 22.) It is not between first network device 14 and originating telephony device 24. (*Id.*)

Likewise, "Inform 114" also cannot be the claimed message because it is not received "at a network address corresponding to the secure name associated with the first device." (*Id.*) Requester alleges that the unique identifier of end-point devices (24, 26) is a "secure name" and that the "private IP addresses . . . assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26)" is a network address corresponding to the secure name. But, as shown in the FIG. 6, "Inform 114" is received by trusted-third-party network device 30 and not by any of end-point devices (24, 26) or first and second network devices (14, 16). The trusted third-party-network device 30 does not correspond to the alleged secure name (*i.e.*, the unique identifier). Thus, "Inform 114" is not received "at a network address corresponding to the secure name associated with the first device." (*Id.*)

For the same reasons, "Negotiate 118" cannot be the claimed message because this also describes communications between one of network devices (14, 16) and trusted-third-party network device 30. (*Id.*) Thus, "Negotiate 118" also is not received "at a network address corresponding to the secure name associated with the first device."

Accordingly, *Beser* does not disclose "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[ ] to securely communicate with the first device," as recited in claim 1.

b. *Beser* Fails to Disclose the Claimed "First Device" and "Second Device"

Claim 1 recites both a "first device" and a "second device" that include certain claimed features. For example, claim 1 recites, among other things:

- receiving, at a network address corresponding to the secure name associated with the *first device*, a message from a *second device* of the desired to securely communicate with the *first device*; and
- sending a message over a secure communication link from the *first device* to the *second device.*

Beser does not disclose a "first device" and a "second device" each including all of these features.

Requester appears to recognize *Beser*'s shortcomings, as it never expressly identifies the elements of *Beser* that it alleges to read on the claimed "first device" and "second device." Instead, Requester mixes and matches features from different *Beser* devices in an attempt to show unpatentability. For example, Requester initially implies that *four* different devices in *Beser* disclose the recited "first device" and "second device." (*See* Request at 25, "First and second network devices (14, 16) and end-point devices (24, 26) have associated therewith both secure and unsecure names.") Then, Requester implies that two of those four devices, end-point devices (24, 26), are the claimed "first device" and "second device." (*See* Request at 29-31, relying on the communication between end-point devices (24, 26) as allegedly disclosing "sending a message over a secure communication link from the first device to the second device.") Thus, the rejection of claim 1, which adopts Requester's position, should be withdrawn because it shows that *Beser* does not disclose the claimed "first device" and "second device" as arranged in the claims. *See Net MoneyIn, Inc.*, 545 F.3d at 1369 ("unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it . . . cannot anticipate under 35 U.S.C. § 102.").

Moreover, no combination of the first and second network devices (14, 16) and end-point devices (24, 26) can be the recited "first device" and "second device." (Keromytis Decl. ¶ 24.) For example, end-point devices (24, 26) cannot be the "first device" and the "second device," because then *Beser* does not disclose "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." (*Id.*) As discussed above, Requester does not point out where *Beser* discloses the recited "message." Of all the communications shown in Fig. 6 of *Beser* that Requester cites as allegedly disclosing the recited "message," none of these communications are between end-point device 24 and end-point device 26. (*See Beser* Fig. 6.) Indeed, *Beser* simply does not disclose that end-point device 24 receives a message from end-point device 26 of the desire to communicate securely with end-point device 24. (Keromytis Decl. ¶ 24.)

Likewise, first network device 14 and second network device 16 also cannot be the recited "first device" and "second device" because the alleged secure communication link (*i.e.*, *Beser*'s tunneling association, Req. at 29-31), is formed between originating telephony device 24 and terminating telephony device 26, and not between first network device 14 and second network device 16. (Keromytis Decl. ¶ 25.)

c. *Beser* Fails to Disclose "Sending a Message over a Secure Communication Link"

Claim 1 recites, among other things, "sending a message over a secure communication link from the first device to the second device." The Office and Requester allege that the tunneling association of *Beser* corresponds to the claimed "secure communication link" because the "tunneling association hides the identity of the originating and terminating ends of the tunneling association from other users of a public network," and because the broadest reasonable interpretation of a secure communication link does not require encryption. (Req. at 28.) This is incorrect because (1) the broadest reasonable interpretation of secure communication link requires encryption, and *Beser*'s tunneling association is not encrypted; and (2) even if the Office determines that a secure communication link does not require encryption, *Beser*'s tunneling association still is not a secure communication link.

(i) The Broadest Reasonable Interpretation of "Secure Communication Link" Requires Encryption

The broadest reasonable interpretation of a secure communication link requires encryption, and one skilled in the art at the time of the invention would have had the same understanding. (*See* Keromytis Decl. ¶ 27.) The '181 patent supports this broadest reasonable interpretation by explaining that "[d]ata security is usually tackled using some form of data encryption." ('181 patent 1:50-57; Keromytis Decl. ¶ 27.) Indeed, encryption is described throughout the '181 patent as providing data security. (*See*, *e.g.*, '181 patent 9:57-58, 11:5-7.) In the context of the claimed secure communication link, the '181 patent states that the secure communication link may be established without the need for a user to manually enter encryption keys, thus demonstrating that encryption is used in the secure communication link. (*See* '181 patent 50:1-3.)

Requester's position that a secure communication link does not require encryption belies the position it has taken in an ongoing litigation between Requester and Patent Owner. During the litigation, Requester has consistently asserted that a secure communication link requires encryption. (*Compare* Ex. A-2 at 10-11 with *id.* at 2 (Requester proposing that "secure communication link" be construed to be the same as a "virtual private network communication link," which Requester also proposes to require encryption)) Requester also recently filed a motion requesting that the district court construe "secure communication link" as "'a direct communication link that provides data security *through encryption*.'" (*See* Ex. A-9 at 2-3.) Requester should not now be allowed to argue that the claimed secure communication link does not require encryption merely because it is convenient for this reexamination.

Beser's tunneling association between the originating and terminating devices is not a secure communication link because communication between these devices is not encrypted. (Keromytis Decl. ¶ 28.) Instead, *Beser* discloses establishing a tunneling association that merely hides the identity of the originating and terminating ends of the tunneling association from other users of a public network. (*Beser* 2:36-40; Keromytis Decl. ¶ 28.) In fact, *Beser* acknowledges encryption, but specifically teaches away from using it because, according to *Beser*, encryption may provide insufficient protection, may be infeasible to implement, and/or may create service problems due to computer-power limitations. (*Beser* 1:54-67; Keromytis Decl. ¶ 28.) Thus, one of ordinary skill in the art, when reading *Beser*, would understand that *Beser*'s tunneling association does not establish a secure communication link, but instead provides an alternative to establishing one. (Keromytis Decl. ¶ 28.)

The Office and Requester also assert that *Beser* discloses using IPsec as "another method of securely communicating." (Req. at 28, citing *Beser* 1:54-56.) But this limited reference to IPsec, which appears in the "background" section of *Beser*, is not disclosed as part of *Beser*'s tunneling association, (Keromytis Decl. ¶ 29), and thus cannot be used to support a rejection under § 102(e). Moreover, as discussed, the "background" section of *Beser* specifically teaches away from using encryption in the configurations disclosed by *Beser*. (*Beser* 1:54-67; Keromytis Decl. ¶ 29.)

(ii) Even if Encryption Is Not Required, *Beser* Still Does Not Disclose a "Secure Communication Link"

Even if the Office were to determine that a secure communication link does not require encryption, *Beser*'s tunneling association still is not a secure communication link. As discussed above, the tunneling association of *Beser* merely hides the identity of the originating and terminating ends from a hacker. (*Beser* 2:36-40; Keromytis Decl. ¶ 30.) But this tunneling does not *secure* those communications from eavesdropping once the originating and terminating ends have been discovered. (Keromytis Decl. ¶ 30.) For example, if a data packet sent over the tunneling association of *Beser* were to be intercepted, it could be examined, and the contents of the packet's data payload viewed. (*Id.*)

The '181 patent specifically distinguishes communications that incorporate "*data security*," and are thus "immune to eavesdropping," from communications that merely "prevent an eavesdropper from discovering that [a] terminal . . . is in communication with [another] terminal." ('181 patent 1:28-40; Keromytis Decl. ¶ 30.) *Beser* is directed to the latter, *i.e.*, to "establish a tunneling association that hides the identity of originating and terminating ends of the tunneling association from the other users of a public network." (*Beser* 2:36-39; Keromytis Decl. ¶ 30.) Consequently, *Beser* does not disclose the *data security* required to form a "*secure* communication link," as recited by claim 1. (Keromytis Decl. ¶ 30.) Thus, *Beser* does not disclose "sending a message over a secure communication link from the first device to the second device" and cannot anticipate claim 1.

For at least the reasons discussed above, the rejection of claim 1 should be withdrawn.

3. Independent Claim 2

Claim 2 recites, among other things, "a secure name service." The Office and Requester allege that trusted-third-party network device 30 in *Beser* is the claimed "secure name service" because trusted-third-party network device 30 "may be a back-end service, domain name server, or the owner/manager of database or directory services." (Req. at 33, quoting *Beser* 4:5-11.) The Office and Requester, however, provide no analysis as to how "a back-end service, domain name server, or owner/manager of database or directory services" discloses a "secure name service." Indeed, these alternative embodiments of the trusted-third-party network device do not disclose a "secure name service" and thus cannot support a rejection under § 102. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758.

Moreover, nothing in *Beser* discloses that trusted-third-party network device 30 is a secure name service that facilitates establishing data security, much less facilitates establishing a secure communication link. (Keromytis Decl. ¶ 31.) For example, *Beser* discloses that its trusted-third-party network device "is connected to the public network," but omits any description of how the trusted-third-party network device is associated with any form of security. (*Beser* 4:1-2; Keromytis Decl. ¶ 31.) Since *Beser* does not disclose a "*secure* name service" of any kind, *Beser* cannot anticipate claim 2.

Additionally, the Office's and Requester's allegation that the tunneling association of *Beser* corresponds to the claimed "secure communication link" falls short for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 2 should be withdrawn.

4. Dependent Claims 3-23

Claims 3-23 depend directly or indirectly from claim 2 and include all of its features. They are patentable for at least the reasons discussed above regarding claim 2. Claims 5-7, 9-11, 18 and 23 further distinguish over *Beser* for the reasons discussed below.

5. Dependent Claim 5

Claim 5 recites, among other things, "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form." The Office and Requester do not allege that the tunneling association of *Beser* includes messages that are encrypted. Rather, the Office Action and Request allege that "encryption can be used" because a background portion of *Beser* references IPSec. (Req. at 36.) First, this limited reference to IPsec is *not* part of the tunneling association of *Beser*, (Keromytis Decl. ¶ 34), and thus cannot be used to support a rejection under § 102. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758. Even so, for reasons similar to those in support of claim 1, *Beser* discloses IPsec and other encryption techniques only to the extent that they should *not* be used in tunneled connections and VoIP applications, the technology with which *Beser* is primarily concerned. (Keromytis Decl. ¶ 34.)

Moreover, with respect to claim 2, from which claim 5 depends, the Office and Requester allege that a portion of *Beser* that recites "the first network device (14) has the following network addresses . . ." discloses the claimed "message containing the network address." (Req. at 35, citing *Beser* 21:38-43.) The cited portion of *Beser*, however, does not disclose receiving a message containing a network address, much less receiving a message in an encrypted form of any kind. (Keromytis Decl. ¶ 35.) Indeed, nothing in *Beser* discloses encryption of a message containing the alleged network address. (*Id.*) Consequently, *Beser* cannot anticipate dependent claim 5.

6. Dependent Claim 6

Claim 6 recites, among other things, "[t]he method according to claim 5, further including decrypting the message." Claim 6 depends from claim 5, includes all of its features, and is therefore patentable for reasons similar to claim 5. With regard to claim 6, the Office and Requester merely allege that "[i]t would be inherent in *Beser* to 'decrypt' the very information that it recommends encrypting." (Req. at 37.) This allegation fails because the rejection has not pointed to a single feature in *Beser* in which decrypting the message would be necessarily present. *Ex parte Schricker*, 56 USPQ2d 1723, 1725 (B.P.A.I. June 7, 2000) (unpublished) ("it is incumbent on the examiner to point to the 'page and line' of the prior art which justifies an inherency theory"). Accordingly, the rejection of claim 6 should be withdrawn.

7. Dependent Claim 7

Claim 7 recites, among other things, "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." The Office and Requester point to a single paragraph in *Beser* that lists several names of standards allegedly compatible with the system of *Beser*, and concludes that the system and methods of *Beser* anticipate claim 7. (Req. at 37.) However, merely reciting a laundry list of standards does not disclose a device "capable of supporting a *secure communication link as well as a non-secure communication link*," or "establishing a non-secure communication link with the second device *when needed*," as recited by claim 7. The Office and Requester do not provide any additional explanation why *Beser* discloses these features by merely reciting the list of standards.

In addition, none of these purported "standards" have properly been incorporated by reference into *Beser* so as to provide sufficient support for a rejection under § 102. *See Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) ("To incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents."). Accordingly, the rejection of claim 7 should be withdrawn.

8. Dependent Claim 9

Claim 9 recites, among other things, "automatically initiating the secure communication link after it is enabled." The Requester alleges that the tunneling association of *Beser* would be established automatically because *Beser* discloses the tunneling association "without reference to user interaction." (Req. at 38.) The Requester, in effect, alleges that *Beser* discloses a feature by remaining silent regarding that very feature. Besides being illogical, this position does not support a case of anticipation because it does not point out how *Beser* discloses "each and every element as set forth in the claim." *Verdegaal Bros.*, 814 F.2d at 631; *see* 35 U.S.C. § 132. Likewise, the Office and Requester have not described what portion of *Beser* discloses that a secure communication link is enabled, and then initialized "after it is enabled," as recited by claim 9. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758. Accordingly, the rejection of claim 9 should be withdrawn.

9. Dependent Claims 10 and 11

Claim 10 recites, among other things, "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 recites, among other things, "receiving the message in the form of at least one tunneled packet." The Office and Requester allege that *Beser* discloses these features by citing to a portion of *Beser* that discusses hiding the IP addresses of the originating and terminating devices inside a payload field during negotiation of a tunneling association. (Req. at 38-39, citing *Beser* 12:6-19.) However, this portion of *Beser* is directed to what Requester alleges to be the secure communication link, not the alleged "message containing the network address." The Office and Requester also allege that the features of claims 10 and 11 are anticipated because *Beser* discloses that tunneling "is accomplished by encapsulating the IP packet to be tunneled within the payload field of another packet that is transmitted on the public network." (*See, e.g.*, Req. at 38, quoting *Beser* 2:9-12.) But this portion of *Beser* is also not directed to the alleged "message containing the network address." Consequently, the cited portions of *Beser* cannot support a rejection of claims 10 and 11 under § 102. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758.

10. Dependent Claim 18

Claim 18 recites, among other things, "wherein the secure communication link is an authenticated link." The Office and Requester cite to a brief disclosure related to encryption and authentication of the alleged secure name (*i.e.*, unique identifier) as corresponding to this feature. However, *Beser* does not disclose that encrypting or authenticating the alleged secure name (*i.e.*, the unique identifier) has anything to do with the alleged secure communication link (*i.e.*, tunneling association). (Keromytis Decl. ¶ 36.) Thus, merely disclosing that the unique identifier can be authenticated does not disclose that the tunneling association is an authenticated link. Consequently, the rejection of claim 18 should be withdrawn. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758.

11. Dependent Claim 23

Claim 23 recites, among other things, "the secure name of the second device is a secure, non-standard domain name." *Beser* does not disclose that the unique identifier (referred to as a "domain name") is a "non-standard domain name." (Keromytis Decl. ¶ 37.) Consequently, *Beser* cannot anticipate claim 23 because "each and every element as set forth in the claim" is not found in *Beser*. *Verdegaal Bros.*, 2 USPQ2d at 1053. For at least this reason, the rejection of claim 23 under § 102(e) should be withdrawn, and the patentability of claim 23 be confirmed.

12. Independent Claim 24

Claim 24 recites, among other things, "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address." The Office and Requester allege that the "unique identifier" (*i.e.*, the alleged secure name) and the "public IP 58 address for the second network device 16" are associated because "the association of the secure name with the terminating device – is only possible because each device (including the originating device) has already requested and obtained registration of its secure name." (Req. at 46.) Hence, the Office and Requester merely assume the alleged first device (*i.e.*, the terminating device) already requested and obtained registration. (*See id.*)

The Office and Requester have conceded that *Beser* does not explicitly disclose at least the feature of "at the first device requesting and obtaining registration of a secure name for the first device." (*See id.*) Without reference to how the claimed feature of "at the first device requesting and obtaining registration of a secure name for the first device" is anticipated, the Office cannot leave Patent Owner to guess what part of *Beser* contains the missing subject matter. *See Ex parte Schricker*, 56 USPQ2d at 1725 ("it is incumbent on the examiner to point to the 'page and line' of the prior art which justifies an inherency theory"). For this reason alone, the rejection under § 102 should be withdrawn. *See id.* at 1725-26; 35 U.S.C. § 132.

Moreover, there is simply no evidence that the claimed feature of "at the first device requesting and obtaining registration of a secure name for the first device" is necessarily present in *Beser* to support an inherency theory. For example, the unique identifier of *Beser* (*i.e.*, the alleged secure name) may be associated with the private IP addresses in any number of ways, including having been encoded into software, provided by an administrator, or transmitted by a device different than the alleged first device. (Keromytis Decl. ¶ 38.) Furthermore, the Office and Requester have not pointed to a single portion of *Beser* that would disclose "requesting" or "obtaining" registration of a secure name for the alleged first device. Consequently, the rejection under § 102 cannot be sustained.

Claim 24 further recites, among other things, "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device." The allegations that this feature is disclosed by *Beser* are identical to those given in the rejection of claim 1, (*compare* Req. at 27-29 *with id.* at 47-48), and *Beser* does not disclose the recited features of claim 24 for reasons similar to those given in support of patentability of claim 1.

Claim 24 also recites "sending a message securely from the first device to the second device." The Office and Requester do not explain how this feature is disclosed by *Beser*. Instead, the Requester's allegations regarding this feature are identical to those presented regarding a "secure communication link" in claim 1. (*Compare* Req. at 30 *with id.* at 49.) For the reasons similar to those discussed above regarding claim 1, the rejection of claim 24 should be withdrawn. Indeed, nothing in *Beser* discloses *securely* sending a message of any kind.

13. Dependent Claim 25

Claim 25 depends from claim 24 so it is patentable for at least the reasons discussed above regarding claim 24. Claim 25 also recites, among other things, "sending the message from the first device to the second device using a secure communication link." The Office's and Requester's analysis of this feature is substantially identical to that given in the rejection of claim 1, (*compare* Req. at 30-31 *with id.* at 50-50), and *Beser* does not disclose the recited feature of claim 25 for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 25 should be withdrawn.

14. Independent Claim 26

Claim 26 recites, among other things, "from the first device requesting and obtaining registration of an unsecured name associated with the first device," "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device," "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device," and "from the first device sending a message securely from the first device to the second device." The allegations regarding these features are substantially identical to those given in the rejection of claim 24, (*compare* Req. at 46-49 *with id.* at 52-55), so *Beser* does not anticipate claim 26 for reasons similar to those given in support of patentability of claim 24.

In addition, the Office and Requester have not pointed to a single portion of *Beser* that would disclose "requesting and obtaining registration of an *unsecured* name." The Requester merely copied its allegations regarding a "secure name" without any mention of how those allegations relate to an "unsecured name." (*See* Req. at 52.) Accordingly, the rejection of claim 26 should be withdrawn. *See* 35 U.S.C. § 132.

15. Dependent Claim 27

Claim 27 depends from claim 26, so it is patentable for at least the reasons discussed above regarding claim 26. Claim 27 also recites, among other things, "using the first device to obtain a registration of the unsecured name associated with the first device," and "using the first device to obtain a registration of the secure name associated with the first device." The Office and Requester have not explained how *Beser* discloses "using the first device" to accomplish the features of claim 27 in the manner claimed. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758. Accordingly, the rejection of claim 27 should be withdrawn.

16. Independent Claim 28

Claim 28 recites, among other things, "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device." The allegations that this feature is disclosed by *Beser* are substantially identical to those given in the rejection of claim 2, (*compare* Req. at 33 *with id.* at 58-59), and *Beser* does not disclose the "secure name service" of claim 28 for reasons similar to those supporting the patentability of claim 2.

Claim 28 further recites, among other things, "sending a message to the network address associated with the secure name of the device using a secure communication link." The allegations that this feature is disclosed by *Beser* are substantially identical to those given in the rejection of claim 1, (*compare* Req. at 34-35 *with id.* at 59-60), and *Beser* does not disclose the "secure communication link" of claim 28 for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 28 should be withdrawn.

17. Independent Claim 29

Claim 29 recites, among other things, "receiving at the network address associated with the secure name of a first device a message from a second device requesting the desire[] to securely communicate with the first device." The Office's and Requester's analysis of this feature is substantially identical to that given in the rejection of claim 1 (*compare* Req. at 27-29 *with id.* at 62-

64), and *Beser* does not disclose this feature of claim 29 for reasons similar to those given in support of patentability of claim 1.

Claim 29 further recites, among other things, "wherein the secure name of the first device is registered" and "sending a message securely from the first device to the second device." The Office's and Requester's analysis of these features is substantially identical to that given in the rejection of claim 24, (*compare* Req. at 46, 48-49 *with id.* at 64-65), and *Beser* does not disclose the recited features of claim 29 for reasons similar to those given in support of patentability of claim 24. Accordingly, the rejection of claim 29 should be withdrawn.

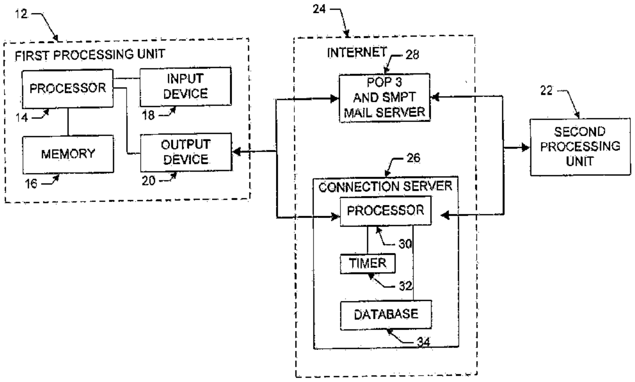
For at least these reasons, claims 1-29 should be confirmed over *Beser*.

C. The Rejection of Claims 1, 2, 6-9, 12-17, 19-21, and 24-29 Under 35 U.S.C. § 102(e) Based on *Mattaway* Should Be Withdrawn (Issue 3)

The Office rejects claims 1, 2, 6-9, 12-17, 19-21, and 24-29 under § 102(e) based on U.S. Patent No. 6,131,121 to Mattaway et al. ("*Mattaway*"). (OA at 5.) For the reasons discussed below, this rejection should be withdrawn and the claims should be confirmed.

1. Overview of *Mattaway*

With reference to Fig. 1, reproduced below, *Mattaway* discloses two embodiments in which a first processing unit (12) sends a query for the network protocol address of a second processing unit (22) and establishes a communication link with the second processing unit upon receipt of the network protocol address. (*Mattaway* Abstract.)



In the first embodiment, *Mattaway* discloses a caller (*i.e.*, first processing unit 12) sending a packet, including an email address of a callee (*i.e.*, second processing unit 22) to a connection server (26) and the connection server returning the IP address of the callee. (*Mattaway* 18:48-64, explaining Fig. 16A.) In the second embodiment, *Mattaway* discloses the caller sending an email, including connection information for the caller, through a mail server (28) to the callee, and waiting for the callee to initiate a connection with the caller using the connection information. (*Mattaway* 7:63-9:15, 8:25-44.)

2. Independent Claim 1

a. *Mattaway* Fails to Disclose "A First Device Associated with a Secure Name and an Unsecured Name"

Claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." The Office and Requester allege that an email address stored on a server is a "secure name" because the server is "protected behind a 'firewall server 1522'" and Table 9 of *Mattaway* discloses an encrypted email address. (Req. at 70, citing *Mattaway* 17:44-48, 40:27.) This interpretation is incorrect.

First, *Mattaway* does not disclose that the email address in Table 9 is associated with any particular device, much less the alleged "callee's device" or any other device allegedly associated with the claimed "first device." (Keromytis Decl. ¶ 44.) *Mattaway* discloses that the data in Table 9 (including the alleged secure name) is returned to a user (*i.e.*, the caller in the cited example) in response to a user "logging on for the first time" to a global server. (*Mattaway* Fig. 17A, 22:65-23:2.) The email address described in Table 9 is not referenced in any other portion of *Mattaway*, and *Mattaway* is completely silent as to the function of the referenced email address and whether it could be associated with a device. (Keromytis Decl. ¶ 44.) In fact, *Mattaway* does not disclose encrypting an email address associated with a device. (*Id.*) Accordingly, characterizing the email address described in Table 9 as the claimed "secure name" is not correct or factually supported.

Second, the firewall of *Mattaway* does not protect email addresses as alleged by the Office and Requester. (Keromytis Decl. ¶ 45.) In fact, if a callee's email address were to be stored on a server behind the firewall (*e.g.*, the global server 1500), that email address would already be known to the caller before the caller connects to the server. (*Id.*) For example, Figure 16A, cited in the Request at pages 70-71, teaches that an email address is received at the global server, *from a caller device*, as part of a <CONNECT REQ> packet. (*Id.*) Similarly, in another example cited in the Request, an email address is sent from a caller to the callee, through a mail server, and the caller waits for a response email. (*Id.*, citing *Mattaway* 7:62-8:35.) In both examples, the email address alleged to be a "secure name" originates from a different location (*i.e.*, a caller device) than what the

Office and Requester point to as providing the alleged security to transform the email address into a "secure name" (*i.e.*, the global server).[3] (*Id.*)

Third, nothing in *Mattaway* discloses or suggests that an email address received by the global server of *Mattaway*, or used by the caller or callee, is a "secure name," much less associated with any security whatsoever. (Keromytis Decl. ¶ 46.) In fact, the terms "secure" or "security," or the like, are completely absent from *Mattaway*. (*Id.*)

Mattaway does not disclose the claimed feature of a secure name, or a first device associated with a secure name. Accordingly, the rejection of claim 1 should be withdrawn.

b. *Mattaway* Fails to Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire[ ] to Securely Communicate with the First Device"

Claim 1 recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." The Office and Requester assert that two different embodiments in *Mattaway* disclose this feature. (Req. at 70-71, citing *Mattaway* Fig. 16A, 8:25-44.) They are incorrect for each embodiment. (*See, e.g.*, Keromytis Decl. ¶ 47.)

In the first cited embodiment, *Mattaway* describes a caller (*i.e.*, first processing unit 12) sending a packet including an email address of the callee to the connection server and the server returning the IP address of the callee. (*Mattaway* 18:48-64, explaining Fig. 16A.) Assuming for the sake of argument that this packet could be a message from a second device, the message is received at the server, and *not* received at what the Office and Requester contend is the "network address corresponding to the secure name" (*i.e.*, the IP address of the callee). (*Id.*; *see also* Req. at 70.)

In the second cited embodiment, the caller sends an email, including connection information for the caller, through a mail server to the callee, and waits for the callee to initiate a connection with the caller using the connection information. (*Mattaway* 7:63-9:15, 8:25-44.) In this embodiment, what the Office and Requester point to as a "secure name" (*i.e.*, an email address) is not stored on what the Office and Requester point to as providing security (*i.e.*, a connection server 26). (*Id.*) The email is sent to a different device altogether (*i.e.*, mail server 28). (*Mattaway* Fig. 1.) Consequently, this embodiment cannot have a "secure name," as described by the Office and Requester. (*Id.*) The

[3] Notably, the email addresses referenced by the preceding examples are *not* disclosed by *Mattaway* as being the previously cited email address of Table 9.

Office and Requester cannot simply pick and choose different features from various embodiments to support a rejection under § 102(e). *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758.

In addition, *Mattaway* does not disclose a "message . . . of the desired to securely communicate." (Keromytis Decl. ¶ 47.) The Office and Requester merely conclude that Figure 16A of *Mattaway* discloses an "intent to securely communicate," but do not point to any explicit passage or provide any reasoning as to how the feature might be inherent. (*Id.*) Accordingly, the rejection is deficient and should be withdrawn. *See In re Rijckaert*, 9 F.3d 1531, 1533, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) ("when the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate <u>where</u> such a teaching or suggestion appears in the prior art") (emphasis added); *Ex parte Schricker*, 56 USPQ2d 1723, 1725 (B.P.A.I., June 7, 2000) (unpublished) ("it is incumbent on the examiner to point to the 'page and line' of the prior art which justifies an inherency theory").

c. *Mattaway* Fails to Disclose "Sending a Message over a Secure Communication Link from the First Device to the Second Device"

Claim 1 recites, among other things, "sending a message over a secure communication link from the first device to the second device." The Office and Requester allege that this feature is disclosed by a reference in *Mattaway* to "point-to-point" Internet communications, and a statement that the WebPhone application of *Mattaway* "enables the parties to converse in real-time, telephone quality, encrypted audio communication." (Req. at 74.) However, the Office and Requester have not explained how these two features in disparate portions of *Mattaway* are "arranged or combined in the same way as recited in the claim," as required by *Net MoneyIN, Inc.*, 88 USPQ2d at 1758. Furthermore, the Office and Requester do not allege or describe what claim feature the recited "encrypted audio communication" corresponds to (*e.g.*, the claimed message, the claimed secure communication link, or some other claimed feature). The Office and Requester also have not alleged or provided any evidence that the claimed feature is necessarily present in *Mattaway* to establish inherency. Accordingly, the rejection of claim 1 is deficient and should be withdrawn.

3. Independent Claim 2

Claim 2 recites, among other things, "from a first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device." The Office and Requester fail to show disclosure of a "secure name service" because, as indicated above, the alleged secure name service (*i.e.*, connection server 26) does not store a "secure name" for the callee's device, as proposed by the Office and Requester. (*See* Req. at 74; *see also*

Keromytis Decl. ¶ 48.) There is simply no evidence that the email address identified in Table 9 is associated with any particular device. (Keromytis Decl. ¶ 48.) In this regard, the allegation that *Mattaway* discloses "a secure name of the second device" is substantially identical to that given in the rejection of claim 1, (*compare* Req. at 70 *with id.* at 74), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 1.

Claim 2 also recites "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." The allegation that *Mattaway* discloses this feature is also substantially identical to the allegations regarding claim 1, (*compare* Req. at 72 *with id.* at 74), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 1.

Accordingly, the rejection of claim 2 should be withdrawn.

4. Dependent Claims 6-9, 12-17, and 19-21

Claims 6-9, 12-17, and 19-21 depend directly or indirectly from claim 2 and include all of its features. They are patentable for at least the reasons discussed above regarding claim 2. Claims 6, 7, 9, and 13 further distinguish over *Mattaway* for the reasons discussed below.

5. Dependent Claim 6

The Office has not adopted the proposed rejection of claim 5, (OA at 5), thus recognizing that Requester has not demonstrated that all of claim 5's features are disclosed in *Mattaway*. Claim 6 depends from claim 5 and therefore includes all the limitations of claim 5. Since claim 5's features are not disclosed in *Mattaway*, *Mattaway* also does not disclose all of the features of claim 6. In any event, Patent Owner is unable to respond to the rejection of claim 6 based on the positions taken in the Office Action, and considers the rejection of claim 6 to be a typographical error where no response is needed. For these reasons, the rejection of dependent claim 6 is deficient and should be withdrawn. *See* 35 U.S.C. § 132.

6. Dependent Claim 7

Claim 7 recites, among other things, "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." Attempting to find this feature, the Office and Requester point to a single sentence in *Mattaway* that states one of two example protocols may be used in establishing communication with a callee processing unit. (Req. at 75, citing *Mattaway* 6:37-45.) However, merely reciting a few example protocol names does not disclose a device "capable of supporting a *secure communication link* ***as well as*** *a non-secure* *communication link*," or "establishing a non-secure communication link with the second device *when needed*," as recited by claim 7. (Keromytis Decl. ¶ 50.) Consequently, the rejection of claim 7 cannot be sustained.

Besides, *Mattaway* does not disclose how the named protocols could be used to effectuate the claimed feature, (*id.*), and neither of the purported "protocols" have properly been incorporated by reference into *Mattaway* so as to provide sufficient support for a rejection. *See Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) ("To incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents."). For this reason, the rejection of claim 7 is deficient and should be withdrawn.

7. Dependent Claim 9

Claim 9 recites, among other things, "automatically initiating the secure communication link after it is enabled." The Office and Requester assert that the alleged secure communication link would be established automatically because "nothing in the specification [of *Mattaway*] suggests user interaction is involved regarding the underlying actions of the computer programs that set up the . . . communications." (Req. at 76.) Hence, the Office and Requester allege that the claimed feature is disclosed by *Mattaway* merely because *Mattaway omits* something that may challenge the presence of the feature. This type of allegation does not indicate to Patent Owner where "each and every element as set forth in the claim" is disclosed, *Verdegaal Bros.*, 814 F.2d at 631, and cannot be a basis for a *prima facie* case of anticipation. *See* 35 U.S.C. § 132. Moreover, the Office has not described what portion of *Mattaway* discloses that a secure communication link is enabled, and then initialized "after it is enabled," as recited by claim 9. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758 (anticipation requires "all of the limitations arranged or combined in the same way as recited in the claim"). For these reasons, the rejection of claim 9 is deficient and should be withdrawn.

8. Dependent Claim 13

Claim 13 recites, among other things, "wherein the receiving and sending of messages through the secure communication link includes multiple sessions." The Office and Requester allege that this feature is disclosed because "each call, *i.e.*, session, 'may be assigned a successive session number . . .'." (Req. at 76, quoting *Mattaway* 6:24-36.) However, *Mattaway* discloses that *each call* receives a new session. (*Mattaway* 6:24-36; Keromytis Decl. ¶ 51.) Since the Office and Requester have taken the position that "point-to-point Internet communications with the callee" that arise from a ***single call*** correspond to the claimed secure communication link, (Req. at 74), the Office and

Requester cannot now allege that the alleged communication link has more than one session. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758. Consequently, the alleged secure communication link does not include "multiple sessions," as recited by claim 13. (Keromytis Decl. ¶ 51.)

9. Dependent Claims 14 and 15

Claim 14 recites, among other things, "supporting a plurality of services over the secure communication link." The Office and Requester allege that this feature is disclosed by the naming of two example datagram services that may be used in establishing communication with a callee processing unit. (Req. at 77, citing *Mattaway* 6:37-45.) However, the mere recitation of a few alternative names does not disclose the claimed "supporting a plurality of services over a secure communication link." *Mattaway* also does not disclose how the named "protocols" could be supported or used to effectuate the claimed feature, and neither of the purported "protocols" have properly been incorporated by reference into *Mattaway* as to provide sufficient support for a rejection under § 102(e). *See Advanced Display Sys., Inc.*, 212 F.3d at 1282.

The Office and Requester further allege that *Mattaway* discloses a "plurality of application programs" and points to a single "WEBPHONE" program that may be executed on a machine that runs one of several operating systems. (Req. at 77, citing *Mattaway* 4:38-41.) However, disclosure of a single program that may be run on various alternative operating systems does *not* disclose, or even relate to, supporting a *plurality* of services over a *secure communication link.* Consequently, the rejection of claim 14 under § 102 cannot be sustained.

Claim 15 recites, *inter alia*, "the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof." Claim 15 is dependent from claim 14, includes all the limitations of claim 15, and is patentable for reasons similar to claim 14.

Accordingly, the rejection of claims 14 and 15 under § 102(e) should be withdrawn, and the patentability of claims 14 and 15 be confirmed.

10. Independent Claim 24

Claim 24 recites, among other things, "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address." The Office and Requester assert that *Mattaway* discloses this feature because *Mattaway* discloses "the first processing unit 12 automatically transmits its associated E-mail address . . . to the connection server 26." (Req. at 80-81, quoting *Mattaway* 6:60-65.) For at least the explanations similar to those described above regarding independent claim 1, *Mattaway* does not disclose or suggest a "secure name." Moreover, automatically transmitting an email address does not evidence disclosure of "requesting and obtaining registration" of the email address, much less of a "secure name." (Keromytis Decl. ¶ 52.) The Office and Requester have also not articulated what in *Mattaway* corresponds to "requesting" and what in *Mattaway* corresponds to "obtaining," or how it takes place "at the first device." *See* 35 U.S.C. § 132.

Claim 24 also recites "receiving at the network address associated with the secure name of the first device a message from a second device of the desired to securely communicate with the first device." The allegations that this feature is disclosed by *Mattaway* are substantially identical to those given in the rejection of claim 1, (*compare* Req. at 70-71 *with id.* at 81-83), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 1.

Claim 24 further recites "sending a message securely from the first device to the second device." The Office and Requester allege that this feature is disclosed by a brief, isolated passage in *Mattaway* reciting that a "WebPhone application enables the parties to converse in real-time, telephone quality, encrypted audio communication." (Req. at 83, quoting *Mattaway* 25:32-34.) However, this passage discloses nothing about whether, much less how, a message may be sent securely, (Keromytis Decl. ¶ 54), and therefore does not meet the level of disclosure required to show anticipation of claim 24. *See Net MoneyIN, Inc.*, 88 USPQ2d at 1758. In particular, this passage does not disclose at least "sending a message securely from the first device to the second device."

Accordingly, the rejection of claim 24 should be withdrawn.

11. Dependent Claim 25

Claim 25 recites, among other things, "wherein sending a message securely comprises sending the message from the first device to the second deice using a secure communication link." The allegation that this feature is disclosed by *Mattaway* is substantially identical to that given in the rejection of claim 1, (*compare* Req. at 30-31 *with id.* at 50-50), and therefore claim 25 is patentable for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 25 should be withdrawn.

12. Independent Claim 26

Claim 26 recites, among other things, "from the first device requesting and obtaining registration of an unsecured name associated with the first device." The Office and Requester on *Mattaway's* disclosure that a "party's name may be stored in a 'personal information directory.'" (Req. at 85.) However, the personal information directory of *Mattaway* is located on what the Office and Requester point to as the first device, (*see* Req. 84-85), and the Office and Requester do not explain how an "alias" or "party's name" stored on the first device evidences disclosure of the claimed feature of "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Assuming for the sake of argument that the "alias" or "party's name" could be stored on a device different from what the Office and Requester point to as the first device, the Office and Requester still cannot evidence disclosure of "requesting and obtaining registration of an unsecured name associated with the first device." The Office and Requester have not even articulated what in *Mattaway* corresponds to the claimed "requesting," or what corresponds to the claimed "obtaining." Indeed, a review of *Mattaway* reveals that at least these features are not disclosed at all. Consequently, the rejection of claim 26 should be withdrawn.

Claim 26 also recites, "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device." For at least the explanations similar to those described above regarding independent claim 1, *Mattaway* does not disclose or suggest a "secure name." Even so, automatically transmitting an email address, even if that email address is subsequently stored in a database, does not evidence disclosure of "requesting and obtaining registration" of that email address, much less a "secure name." The Office and Requester have not articulated what in *Mattaway* corresponds to "requesting" and what in *Mattaway* corresponds to "obtaining." *See* 35 U.S.C. § 132.

Claim 26 further recites, "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device," and "from the first device sending a message securely from the first device to the second device." The allegations that these features are disclosed by *Mattaway* are substantially identical to those given in the rejection of claim 24, (*compare* Req. at 81-83 *with id.* at 85-87), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 24. Accordingly, the rejection of claim 26 should be withdrawn.

13. Dependent Claim 27

Claim 27 depends from claim 26, includes all of its features, and is patentable for at least the reasons discussed above for claim 26. Accordingly, the rejection of claim 27 should be withdrawn.

14. Independent Claim 28

Claim 28 recites, among other things, "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device." The Office and

Requester do not specify how *Mattaway* discloses the claimed "secure name of a device" or "secure name service," and, for that reason alone, the rejection of claim 28 is deficient and should be withdrawn. Even so, *Mattaway* does not disclose a "secure name of a device" at least for reasons similar to those given in support of patentability of claim 1, and does not disclose the feature of "a secure name service" at least for reasons similar to those given in support of patentability of claim 2.

Claim 28 also recites, "sending a message to the network address associated with the secure name of the device using a secure communication link." The allegation that this feature is disclosed by *Mattaway* is similar to that given for the "secure communication link" of claim 1, (*compare* Req. at 72 *with id.* at 90), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 28 should be withdrawn.

15. Independent Claim 29

Claim 29 recites, among other things, "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desire to securely communicate with the first device, wherein the secure name of the first device is registered." The allegation that this feature is disclosed by *Mattaway* is substantially identical to that given in the rejection of claim 1, (*compare* Req. at 70-71 *with id.* at 92-94), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 1. Additionally, the Office and Requester do not specify how *Mattaway* discloses "wherein the secure name of the first device is registered," and, for that reason alone, the rejection of claim 29 is deficient and should be withdrawn. *See* 35 U.S.C. § 132.

Claim 29 further recites, "sending a message securely from the first device to the second device." The allegation that this feature is disclosed by *Mattaway* is substantially identical to that given in the rejection of claim 24, (*compare* Req. at 83 *with id.* at 94), and *Mattaway* does not disclose this feature for reasons similar to those given in support of patentability of claim 24. Accordingly, the rejection of claim 29 should be withdrawn.

For at least the reasons discussed above, all anticipation rejections based on *Mattaway* should be withdrawn and claims 1, 2, 6-9, 12-17, 19-21, and 24-29 should be confirmed.

D. The Rejection of Claims 3, 4, 10, 11, 18, and 23 Under 35 U.S.C. § 103 Based on *Mattaway* in View of *Beser* Should Be Withdrawn (Issue 4)

1. Dependent Claims 3 and 4

Claims 3 and 4 depend from claim 2, so they include all of claim 2's features. The Office and Requester do not allege that *Beser* makes up for the deficiencies noted above regarding

Mattaway's disclosure, (*see* Req. at 95-96), so claims 3 and 4 are patentable over *Mattaway* and *Beser*, alone or in combination, for at least the reasons discussed above regarding claim 2.

2. Dependent Claims 10 and 11

Like claims 3 and 4, claims 10 and 11 depend from claim 2 and are patentable over *Mattaway* for the reasons discussed above. The Office and Requester do not allege the *Beser* cures the deficiencies noted above regarding *Mattaway's* disclosure (*see* Req. at 96-97), so they have not demonstrated that the combination of *Mattaway* and *Beser* renders obvious claims 10 and 11.

Claim 10 recites, among other things, "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 recites, among other things, "receiving the message in the form of at least one tunneled packet."

The Office and Requester point to *Mattaway's* statement that the WebPhone application "enables the parties to converse in real-time, telephone quality, encrypted audio communication," and then allege that a person skilled in the art would have recognized "the beneficial use of tunneling disclosed by *Beser*." (Req. at 96.) As explained in support of claim 1, however, the Office and Requester do not explain what an "encrypted audio communication" is or how it allegedly discloses the claimed features.

With regard to claim 2, from which this claim depends, the Office and Requester allege that *Mattaway* discloses the feature of a "message containing the network address" because connection server 26 sends an IP address of the caller to the first processing unit 12, (Req. at 74, citing *Mattaway* 7:32-37), and that *Beser* also discloses the feature because *Beser* states "the first network device (14) has the following network addresses . . . ," (Req. at 35, citing *Beser* 21:38-43). Neither of these alleged "messages," however, are received *through* the alleged "secure communication link" in the respective references.

The Office and Requester simply have not explained how or why one of ordinary skill in the art would have incorporated *Beser's* alleged tunneling mechanism into *Mattaway's* system. (*See* Req. at 96-97.) Consequently, the rejections of claims 10 and 11 are deficient and should be withdrawn. *See KSR*, 82 USPQ2d at 1396 (citing *In re Kahn*, 441 F.3d at 988) ("there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

3. Dependent Claim 18

Claim 18 recites, among other things, "wherein the secure communication link is an authenticated link." The Office and Requester point to a brief passage in *Beser* related to authenticating the alleged secure name (*i.e.*, the user identifier), and then allege that a person skilled in the art would have recognized using that form of authenticating in the alleged secure communication link of *Mattaway*. (Req. at 98.) However, *Beser* does not explain that encrypting or authenticating the alleged secure name (*i.e.*, the unique identifier) has anything to do with the alleged secure communication link (*i.e.*, tunneling association) in *Beser*, and therefore it cannot be combined with the alleged secure communication link of *Mattaway*. (Keromytis Decl. ¶ 56.) The two features that the Requester wishes to combine are applicable to different mechanisms within their respective references. (*Id.*) The Office and Requester have not articulated any reason why a skilled artisan would have thought to combine the authentication of *Beser* with the alleged secure communication link of *Mattaway*. Consequently *Beser* cannot be properly combined with *Mattaway* to render obvious the claimed feature of "wherein the secure communication link is an authenticated link," and the rejection under § 103 should be withdrawn.

4. Dependent Claim 23

Claim 23 recites, among other things, "the secure name of the second device is a secure, non-standard domain name." The Office and Requester allege that a person skilled in the art would have recognized "the beneficial use of secure, non-standard domain names disclosed by *Beser*." (Req. at 98.) *Beser*, however, does not disclose a *secure, non-standard* domain name for the reasons similar to those discussed above with regard to the rejection of claim 23 under § 102(e) in view of *Beser*. (*See* Section III.B.11; *see also* Keromytis Decl. ¶ 37.) Accordingly, the rejection of claim 23 should be withdrawn.

E. The Rejection of Claims 10 and 11 Under 35 U.S.C. § 103 Based on *Mattaway* in View of *RFC 2401* Should Be Withdrawn (Issue 5)

Like claims 3 and 4, claims 10 and 11 depend from claim 2 and are patentable over *Mattaway* for the reasons discussed above. They are also patentable for the following reasons.

Claim 10 recites, among other things, "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 recites, *inter alia*, "receiving the message in the form of at least one tunneled packet." The Office Action and Requester allege that these features are rendered obvious because a person skilled in the art would have "recognized the beneficial use of secure, tunneling disclosed by *RFC 2401* would have been equally useful to those methods already described by *Mattaway*." (Req. at 99, 100.)

However, with regard to claim 2, the Office and Requester allege that the claimed "message containing the network address" corresponds to the connection *server* of *Mattaway* sending an IP address to the first processing unit 12, and the claimed "secure communication link" corresponds to "point-to-point Internet communications" between first processing unit 12 and a *callee*. (*See* Req. at 74.) Given this interpretation, the alleged message is not received *through* the alleged "secure communication link."

RFC 2401 is directed to IPsec, a suite of security protocols, and therefore does not remedy the deficiencies of *Mattaway*. Accordingly, the features of claims 10 and 11 cannot be rendered obvious by *Mattaway* or *RFC 2401*, alone or in combination. *See Ex Parte Karl Burgess*, Appeal 2008-2820, 2009 WL 291172, at *3. Accordingly, the rejection of claims 10 and 11 under § 103 should be withdrawn, and the patentability of claims 10 and 11 be confirmed.

F. The Rejection of Claims 1-9, 12-15, 18-29 Under 35 U.S.C. § 102(b) Based on *Lendenmann* Should Be Withdrawn (Issue 6)

The Office rejects claims 1-9, 12-15, and 18-29 under 35 U.S.C. § 102(b) based on *Lendenmann*. As discussed below, however, these rejections should be withdrawn.

1. Overview of *Lendenmann*

Lendenmann discloses a distributed computing environment ("DCE"), which "is a layer of services that allows distributed applications to communicate with a collection of computers, operating systems, and networks." (*Lendenmann* 7.) As illustrated in Figure 3, *Lendenmann*'s DCE may include several different components, including security services, time services, and directory services. (*Id.* at 8.)

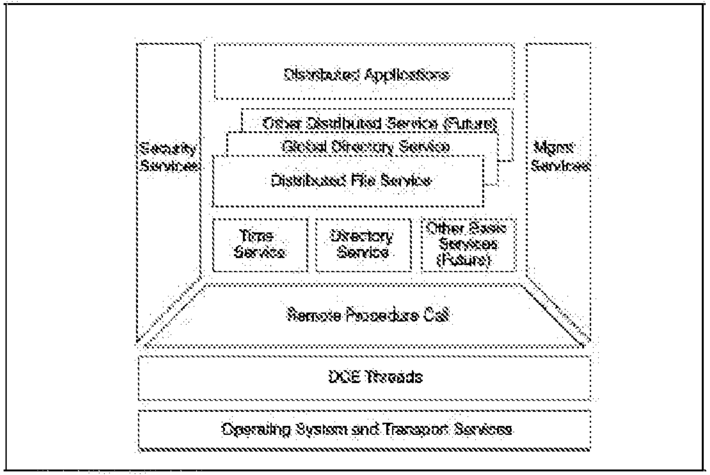


Figure 3. DCE Architecture

(*Id.*) It further discloses that a collection of machines, operating systems, and networks managed by a single set of DCE services constitutes a "DCE cell." (*Id.*) At a minimum, a cell must contain a Security Server, a Cell Directory Server ("CDS"), and Distributed Time Servers. (*Id.* at 9.) These separate components provide different services for establishing remote procedure calls ("RPCs") between clients and servers.

RPCs between clients and servers may or may not employ security features, such as authentication and encryption. (*See, e.g.*, *id.* at 192.) Whether an RPC utilizes security features lies completely within the discretion of the client. (*Id.* at 71, 192.) A client may select the desired security level only after obtaining a binding handle containing a network address for a server, as the server must also be able to support the designated security features. (*Id.* at 71, 207-08.) For interoperability purposes, *Lendenmann*'s DCE supports two naming schemes for organizing server network addresses: X.500 and DNS. (*Id.* at 21.) These binding handles, available from several different sources, also contain various other information necessary for the client to connect to a server during the RPC process, including, for example, object UUIDs, protocol sequences, and endpoints. (*Id.* at 182-84.)

To locate a server to remotely provide services or applications over the DCE, a client searches for servers during the "binding" process. (*Id.* at 182.) A client must first decide on a binding method, and *Lendenmann* describes three alternatives: automatic, implicit, or explicit binding. (*Id.* at 180.) A client then must locate servers, for which *Lendenmann* also describes several alternatives: searching files, environment variables, or the CDS; or simply hard-coding a network address into an application. (*Id.* at 182.) A client then obtains binding handles from various possible sources, such as the server RPC runtime, the server host DCE daemon, the CDS, or the client RPC runtime. (*Id.* at 182-83.) These binding handles each identify a server to the client. (*Id.* at 182.) Because *Lendenmann*'s clients search for compatible servers that "handle[] the interface that the client is interested in," (*id.*), a client might receive binding handles for several compatible servers. (*Id.* at 185, describing the process of obtaining binding handles from the CDS.) Upon choosing an appropriate binding handle, the client may select supported security features, call the server, and establish an RPC. (*See id.* at 207-08, "Putting It All Together.")

2. Independent Claim 1

Independent claim 1 recites a number of features that are not taught by *Lendenmann*, as discussed below.

a. *Lendenmann* Fails to Disclose "A First Device Associated with a Secure Name and an Unsecured Name"

Independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." *Lendenmann* does not disclose these features.

The Office and Requester assert that *Lendenmann* discloses this feature because of the "distinction between the X.500 and DNS naming conventions," namely that X.500 is secure, while DNS is unsecured. (OA at 7; Req. at 102, identifying X.500 names as secure names; *id.* at 105-06.) This is incorrect because *Lendenmann* simply presents X.500 and DNS as two alternative DCE-compatible general naming schemes for organizing network addresses: "X.500 is an emerging global directory service standard, but the Internet domain name system (DNS) is an established industry standard. For interoperability purposes, GDS supports both X.500 and DNS transparently." (*Lendenmann* 21.)

The Requester attempts to support its assertions by highlighting two differences between the DNS and X.500 schemes, but it fails to explain how these differences suffice to make X.500 "secure" and DNS "unsecured." (Req. at 105.) The Requester first asserts that Figure 10, reproduced below, somehow reveals the secure/unsecure distinction between X.500 and DNS.

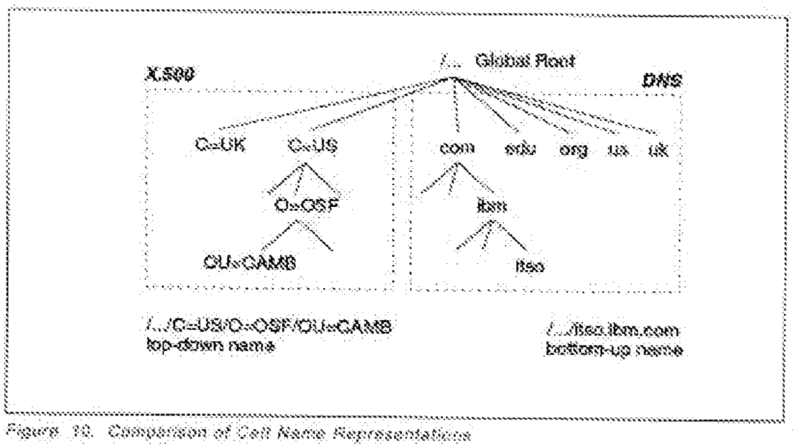


Figure 10. Comparison of Cell Name Representations

Figure 10 shows a comparison of the DNS hierarchical tree structure and the X.500 CDS representation. X.500 picks the names in a top-down order, while DNS does it in bottom-up order.

(Req. at 106; *Lendenmann* 24.) As *Lendenmann* explains in the caption, Figure 10 simply illustrates an organizational difference between X.500 and DNS. (*Lendenmann* 24.) X.500 organizes names in a "top-down" order, while DNS organizes names in a "bottom-up" order. (*Id.*) *Lendenmann* does not disclose how or why these organizational differences would render X.500 "secure" and DNS "unsecured," and the Requester does not even attempt to explain the relationship between organizational structure and security, instead vaguely asserting that "the distinction . . . can be distilled" from Figure 10. (Req. at 106; *see also* Keromytis Decl. ¶ 61.) This cannot support the rejection under 35 U.S.C. § 102(b), as the Requester fails to explain how *Lendenmann* either expressly or inherently discloses this feature of claim 1. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) ("the proponent must show 'that the four corners of a single, prior art document describe every element of the claimed invention.'") (internal citations omitted).

Second, the Requester explains that DNS is unsecured because it has "global addressing and routing," whereas X.500 is secure because it is an "internal naming convention" implemented with a service (GDS) that "can store any kind of object." (Req. at 105, quoting *Lendenmann* 23.) But *Lendenmann* specifically requires a "global network routing mechanism" to access foreign cells on the Internet, "[t]he only well-established, multi-vendor-supported global network today." (*Lendenmann* 23; Keromytis Decl. ¶ 62.) *Lendenmann*'s distributed computing environment specifically uses GDS (and thereby X.500) for storing "Internet addresses." (*Lendenmann* 23.) Accordingly, with either X.500 or DNS, "access to the foreign cell *is established over the Internet in both cases*." (*Id.*) Thus, *Lendenmann* illustrates that in its disclosed distributed computing environment, X.500 and DNS perform the same functions, and are simply alternative DCE-compatible naming schemes. (*Id.* at 21-23; Keromytis Decl. ¶ 62.)

Indeed, regardless of whether a user attempts to obtain a network address based on an X.500 name or a DNS name, a user cannot access the CDS at all unless the user is first cleared by the Security Service. (*Lendenmann* 34; Keromytis Decl. ¶ 63.) The Security Service thus weeds out unauthorized users without regard to the naming scheme employed by each user (X.500 or DNS). (*Lendenmann* 34; Keromytis Decl. ¶ 63.) *Lendenmann* does not provide for any second layer of protection in its CDS directory service, and certainly does not disclose any such additional layer of protection based on naming scheme. (Keromytis Decl. ¶ 63.) Nor does the Requester assert that it does. (*See* Req. at 102-06.) The Requester's strained argument to read "secure" and "unsecured" naming features into *Lendenmann* therefore fails.

Furthermore, to the extent the Requester implies that *all* names retrievable from a CDS are "secure" names, it does so contrary to the clear teachings of *Lendenmann*. *Lendenmann* does not disclose, and the Requester does not identify, any security-related procedures or results that stem from employing an X.500 name or a DNS name in establishing RPCs—the feature of *Lendenmann* allegedly corresponding to the "secure communication link" of claim 1. (*See* Req. at 106-09; Keromytis Decl. ¶ 64.) Rather, *Lendenmann* expressly teaches that implementation of any security features during RPCs lies within the complete discretion of the user-client, regardless of the naming convention employed. (*Lendenmann* 71, "RPC clients *may choose* a security level they want to use. Of course, the level they choose must match a level supported by the server," emphasis added; Keromytis Decl. ¶ 64.) Indeed, "[w]hen a client establishes authenticated RPC, it *can specify* the level of protection to be applied to its communication with the server," including "None." (*Lendenmann* 192, emphasis added; Keromytis Decl. ¶ 64.) Thus, any security-related aspects of *Lendenmann* are independent of the decision to use X.500 names or DNS names. (Keromytis Decl. ¶ 64.) Accordingly, X.500 and DNS names are neither "secure" nor "unsecured," so the rejection based on *Lendenmann* should be withdrawn. (*Id.*)

b. *Lendenmann* Fails to Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device"

Independent claim 1 recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device." *Lendenmann* does not disclose this feature.

In contrast to the Requester's assertions, as discussed above, *Lendenmann* fails to disclose that X.500 names are "secure" in any fashion. Therefore, *Lendenmann* cannot disclose that any action occurs with respect to a "network address corresponding to the *secure* name associated with the first device," much less receiving "a message from a second device." Accordingly, *Lendenmann* does not disclose the "receiving" feature of claim 1.

Even if one were to incorrectly assume that an X.500 name corresponds to a "secure name," the Requester does not identify any passage in *Lendenmann* describing receiving any message at a network address corresponding to an X.500 name instead of a DNS name. (Keromytis Decl. ¶ 65.) The Requester identifies *Lendenmann*'s RPC runtime call to a server as the "message" of claim 1, in which *Lendenmann* explains that a client's RPC runtime may search for addresses to include in its binding information to send to a server. (Req. at 107-08; *Lendenmann* 182, 186-87.) But nowhere does *Lendenmann* describe including X.500 addresses in the binding information, much less any security-related consequences of utilizing X.500 names versus DNS names. (*See, e.g.*, *id.* at 190, describing the process of "1. Looking up a binding in CDS." *See also* Keromytis Decl. ¶ 65.)

For at least these reasons, *Lendenmann* does not disclose the features of claim 1, so the rejection should be withdrawn.

3. Independent Claim 2

Lendenmann does not disclose at least the following features of claim 2.

a. *Lendenmann* Fails to Disclose "a Second Device Having a Secure Name"

Independent claim 2 recites, among other things "[a] method of using a first device to communicate with *a second device having a secure name*" (emphasis added). *Lendenmann* does not disclose this feature because, as discussed above regarding claim 1, *Lendenmann* does not disclose any "secure" names. Thus, *Lendenmann* does not anticipate claim 2.

b. *Lendenmann* Fails to Disclose "a Secure Name Service"

Independent claim 2 recites, among other things, "a secure name service." *Lendenmann* does not disclose this feature. The Office and Requester assert that the CDS is a secure name service because the DCE's Security Service controls access to the CDS by requiring authentication and authorization before the CDS completes any name-service operations. (OA at 7; Req. at 112-13.) This is incorrect.

The CDS is not a "secure name service" because it has no bearing whatsoever on whether the communications for which it provides network addresses are secure or not. (Keromytis Decl. ¶¶ 66-67.) As disclosed and claimed in the '181 patent, a "secure name service" is a service that both resolves a secure name into a network address and further supports establishing a secure communication link. (Keromytis Decl. ¶ 66.) The CDS's role, however, is limited to providing binding information. (*Lendenmann* 207-08, describing the overall RPC process.) The security features for RPC, if any, are incorporated only *after* the client has finished obtaining the necessary binding information: "After the client has the binding handle, it can add to it the desired security level for the RPC calls. Then it issues an RPC . . . ." (*Id.* at 208; Keromytis Decl. ¶ 66.) Thus, *Lendenmann* explains that the CDS's role in RPC is finished before any security measures are invoked within the discretion of the user. (*Lendenmann* 207-08; *id.* at 192, explaining that a client can in fact specify "[n]o communication protection[s].")

Because the CDS has no bearing on whether the communications for which it provides network addresses are secure, the CDS performs no functions beyond those that the '181 patent recognizes and distinguishes as being conventional name services. (Keromytis Decl. ¶ 67.) For example, the conventional name service described in the '181 patent, similar to the CDS, does nothing more than return server-identifying information, such as an IP or network address. (*See, e.g.*, '181 patent 38:54-56.) By contrast, the '181 patent distinguishes its inventive name services, such as the "secure name service" recited in claim 2, as those that do not simply return an IP address but also further support establishing a secure communication link, such as by "automatically set[ting] up a virtual private network between the target node and the user." (*Id.* at 39:30-31.) As the '181 patent teaches, whether such security features are ultimately employed depends precisely on whether the name of the target server is "secure" or not, unlike with *Lendenmann*'s CDS and RPC procedures, as discussed above. (*Id.* at 39:53-40:14.) Thus, *Lendenmann*'s CDS does not disclose a "secure name service," as recited in claim 2.

c. *Lendenmann* Fails to Disclose "from the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated with the Secure Name of the Second Device"

Independent claim 2 recites, among other things, "from the first device, sending a message to a secure name service, *the message requesting a network address associated with the secure name of the second device*" (emphasis added). *Lendenmann* does not disclose these features.

The Office and Requester contend that a client's requesting a network address for a server during the "binding" process corresponds to the "message" recited in claim 1. (OA at 7; Req. at 112.) This is incorrect. *Lendenmann*'s binding process does not disclose "requesting a network address" associated with any server name at all, let alone a "secure" name. (Keromytis Decl. ¶ 68.) Although *Lendenmann* generically describes that its CDS may return a network address upon receiving a name, (*Lendenmann* 21), this does not apply to interactions between a client and the CDS during the binding process. (*Id.* at 33, explaining that "[t]he RPC client uses the Name Service Interface (NSI) API to get binding information from the CDS"; *id.* at 186, discussing the NSI.) Rather, within the binding process, *Lendenmann* only discloses clients locating services based on criteria *other than server names* during the binding process. (*See, e.g.*, *id.* at 186-87, NSI and "Searching The Namespace"; Keromytis Decl. ¶ 68.) For example, as *Lendenmann* explains and the Request quotes, "[a] client can find a server by asking the CDS for the location of *a server that handles the interface that the client is interested in*," not the location of a server having any particular name. (*Lendenmann* 182; Keromytis Decl. ¶ 68.) Similarly, *Lendenmann* discloses that "[w]hen a client wants to connect to a server, it needs to find a *compatible server*," not one associated with any particular server name. (*Lendenmann* 185, emphasis original.) *Lendenmann*'s RPCs, appropriately described as "function calls," are designed to find servers based on functional criteria to provide services (*e.g.*, applications) from remote locations in the distributed computing environment—not to find servers associated with a particular server name. (*Lendenmann* 172; Keromytis Decl. ¶ 68.)

Indeed, rather than the client in *Lendenmann* providing a name to a name service to identify a server, "[b]inding information includes a set of data that *identifies a server to a client*." (*Lendenmann* 182, emphasis added; Keromytis Decl. ¶ 69.) Therefore, "when the client looks for binding handles, it might obtain handles to *several compatible servers*," *i.e.*, not one associated with any particular name. (*Lendenmann* 185, emphasis added; Keromytis Decl. ¶ 69.) The NSI performs these server-identification functions for the client, and *Lendenmann* teaches that the NSI provides mechanisms for "search[ing] server entries for a compatible server." (*Lendenmann* 186; Keromytis Decl. ¶ 69.) The existence of these mechanisms to search among various compatible servers or to obtain binding information as a means of identifying a server to the client indicate to one of ordinary skill in the art that *Lendenmann* does not disclose a client providing a server name to look up a network address, as alleged by Requester, because the identity of the desired server would have already been known from the server name. (Keromytis Decl. ¶ 69.)

Thus, *Lendenmann* fails to disclose "sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device," as recited in claim 2.

d. *Lendenmann* Fails to Disclose "From the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated with the Secure Name of the Second Device" and "at the First Device, Receiving a Message Containing the Network Address Associated with the Secure Name of the Second Device"

Claim 2 recites, among other things, "sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device," and "at the first device, receiving a message containing the network address associated with the secure name of the second device." *Lendenmann* does not disclose these features for the reasons discussed below.

For establishing RPCs, *Lendenmann* explains that server network addresses are contained in "binding handles." (*Lendenmann* 182-84, "Network address.") As discussed above, *Lendenmann* describes its binding process as not returning any particular network address based on a server name, but rather searching for compatible servers and returning binding handles for "several compatible servers." (*See Lendenmann* 182, 185; Keromytis Decl. ¶ 68.) Thus, for the reasons discussed above, *Lendenmann* neither discloses "sending . . . the message requesting a network address *associated with the secure name* of the second device," nor "receiving a message containing the network address *associated with the secure name* of the second device," and therefore the rejection of claim 2 should be withdrawn, and its patentability confirmed.

Even if one were to incorrectly assume that *Lendenmann* discloses one or more of these features, a person of ordinary skill nevertheless would not have understood *Lendenmann* to disclose the features *as arranged in the claim* due to the extraordinary amount of improper picking and choosing of various features that would be required to arrive at the result asserted in the Request. To anticipate, "[t]he [prior art] reference must clearly and unequivocally disclose the claimed [invention] or direct those skilled in the art to the [invention] without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference." *Net MoneyIN, Inc.*, 545 F.3d at 1371 (quoting *In re Arkley*, 455 F.2d 586, 587 (C.C.P.A. 1972)). However, even if picking and choosing were a permissible line of argument, the Office and Requester have not even attempted to show how one of ordinary skill in the art would have navigated *Lendenmann's* complex sequence of options to achieve the claimed invention. (*See* OA at 7; Req. at 112.) Accordingly, the rejection should be withdrawn.

e. *Lendenmann* Fails to Disclose "Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

Independent claim 2 recites, among other things, "sending a message to the network address associated with the secure name of the second device using a secure communication link." As discussed above for claim 1, *Lendenmann* does not disclose any "secure" or "unsecured" names, nor any security-related differentiation between using X.500 and DNS names. Therefore, *Lendenmann* does not disclose this feature of claim 2.

Nevertheless, if one incorrectly assumes that *Lendenmann* discloses "secure" names, *Lendenmann* does not disclose that its RPC-related security features—alleged to correspond to the claimed "secure communication link"—have anything to do with the allegedly secure (X.500) or unsecured (DNS) names. (Req. at 114-15, merely listing various protection levels disclosed in *Lendenmann.*) To the extent Requester implies that use of X.500 names is inherent in these RPC features, it is not necessarily the case that *Lendenmann*'s system would utilize X.500 names during security-enhanced communications. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (for inherency, the missing descriptive matter must be "*necessarily* present in the thing described in the reference, and . . . would be so recognized by persons of ordinary skill") (emphasis added). Instead, *Lendenmann*'s DNS and X.500 names are security-independent and are provided merely as alternative DCE-compatible naming schemes "[f]or interoperability purposes." (*Lendenmann* 21, 71, 192; Keromytis Decl. ¶ 70.) *Lendenmann's* security features are left in the complete discretion of its user-clients, as discussed above. (*Id.*)

The Office and Requester have not demonstrated that each and every element of claim 2 is expressly or inherently disclosed in *Lendenmann*, so the rejection should be withdrawn.

4. Dependent Claims 3-9, 12-15, and 18-23

Claims 3-9, 12-15, and 18-23 depend directly or indirectly from claim 2 and include all of its features. They are patentable for at least the reasons discussed above regarding claim 2. Claims 5, 6, and 21 further distinguish over *Lendenmann* for the reasons discussed below.

5. Dependent Claims 5 and 6

Claims 5 and 6 directly or indirectly depend from claim 2 so they are patentable for the same reasons as claim 2. Claims 5 and 6 also distinguish over *Lendenmann* because *Lendenmann* does not disclose claim 5's "wherein receiving the message containing the network address associated with the secure name of the second device includes *receiving the message in encrypted form*," or claim 6's "decrypting the message."

The Office and Requester assert that *Lendenmann* discloses these features because it allegedly describes querying the CDS for binding information via encrypted communications and subsequently decrypting the CDS's response. (OA at 7; Req. at 117-21.) In support of these assertions, Requester cobbles together short excerpts gathered from throughout *Lendenmann* without regard to whether they reflect the actual role that *Lendenmann* describes for the CDS in establishing RPCs. (Req. at 117-21, citing *Lendenmann* 21, 34, 57, 182, 186, 192). These assertions are incorrect and fail to support the rejection of claims 5 and 6. *Net MoneyIN, Inc.*, 545 F.3d at 1371 ("[T]he [prior art] reference must clearly and unequivocally disclose the claimed [invention] or direct those skilled in the art to the [invention] without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference.").

In particular, *Lendenmann* discloses a far different role for the CDS in establishing RPCs than the Requester's strained effort to imply that the client and the CDS might themselves communicate via encrypted RPC. (Keromytis Decl. ¶ 72.) Indeed, nowhere does *Lendenmann* disclose that utilizing a CDS in establishing an RPC between a client and a server might first involve establishing an encrypted RPC between the client and the CDS. (*See Lendenmann* 173, "This chapter [10] discusses all components involved in the execution of an RPC, including CDS and Security Services"; *see also id.* at 33, "CDS Lookup." *Lendenmann* provides some security measures to protect a client's accessing of information in the CDS, but these measures notably exclude encryption: "The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is *authenticated and authorized* by the Security Service." (*Lendenmann* 34; Keromytis Decl. ¶ 72.)

Because *Lendenmann* discloses no encrypted communications between a client and the CDS, it cannot and does not disclose "receiving the message in encrypted form," as recited in claim 5. It therefore also does not disclose the "decrypting" feature of claim 6, because *Lendenmann* discloses no communications from the CDS that a client would need to decrypt. The encryption/decryption keys Requester improperly cited outside of the context of the binding process for establishing RPCs fail to support the rejection so the rejection should be withdrawn.

6. Dependent Claim 21

Claim 21 depends from claim 2 so it is patentable for at least the reasons discussed above regarding claim 2. Claim 21 also recites additional features not disclosed in *Lendenmann*, namely "further including providing an unsecured name associated with the device." As discussed above, *Lendenmann* does not disclose any secure or unsecured names, and therefore *Lendenmann* cannot disclose "providing an unsecured name," as recited in claim 21. Furthermore, *Lendenmann* does not disclose that its CDS may provide both a *network address* corresponding to an X.500 name (an allegedly secure name) *and a DNS name itself* (an alleged unsecured name) to the claimed "first device." Nor does Requester assert that it does. (*See* Req. at 127.) Rather, *Lendenmann* explains that X.500 and DNS names are used in the alternative to each other, not that they are both used simultaneously. (*Lendenmann* 24; Keromytis Decl. ¶ 73.) Accordingly, the rejection of claim 21 should be withdrawn.

7. Independent Claim 24 and Dependent Claim 25

The Office and Requester, having earlier asserted with respect to claims 1 and 2 that X.500 names are "secure" while DNS names are "unsecured," now change their position by asserting that *all* names stored within the CDS are "secure," whether X.500 or DNS. (OA at 7; Req. at 134.) As its basis for this drastic expansion in its position, Requester explains that the Security Service must authenticate and authorize a user before the CDS completes any name-service operations. (Req. at 134, citing *Lendenmann* 23.)

But Requester's assertion that *all* names within the CDS namespace are "secure" is contrary to the clear teachings of *Lendenmann*, which expressly teaches that implementation of any security features during RPCs lies within the complete discretion of the user-client. (*Lendenmann* 71, "RPC clients *may choose* a security level they want to use. Of course, the level they choose must match a level supported by the server," emphasis added; Keromytis Decl. ¶ 74.) Indeed, "[w]hen a client establishes authenticated RPC, it *can specify* the level of protection to be applied to its communication with the server," including "None." (*Lendenmann* 192, emphasis added; *see also id.* at 207-08, "After the client has the binding handle, it can add to it the desired security level for the RPC calls. Then it issues an RPC . . . ."; Keromytis Decl. ¶ 74.) Thus, as discussed above for claims 1 and 2, the names stored in the CDS are security-independent so they are neither "secure" nor "unsecured." (Keromytis Decl. ¶ 74.)

Given that *Lendenmann* does not disclose "secure" names, it does not disclose the multiple instances of "secure" names recited in claim 24. Thus, the rejection of claim 24 should be withdrawn. And since claim 25 depends from claim 24 and incorporates all of its features, claim 25 is patentable for the same reasons.

8. Independent Claim 26 and Dependent Claim 27

Like claim 1, independent claim 26 recites multiple instances of "secure" and "unsecured" names. This feature is not disclosed in *Lendenmann* for the same reasons discussed above regarding claim 1. Claim 26 also recites "requesting and obtaining registration of a secure name associated with the first device, *wherein a unique network address corresponds to the secure name associated with the first device*," (emphasis added). Requester cites a portion of *Lendenmann* that generically describes "registering servers in the namespace," but neither this passage nor any other in *Lendenmann* discloses that a server may be registered with an additional "unique network address" corresponding to another name, much less a "secure" name. (Req. at 142, citing *Lendenmann* 203.) Requester additionally fails to explain how *Lendenmann* inherently discloses any such feature, as nothing in *Lendenmann* requires that allegedly "secure" X.500 names must *necessarily* correspond to unique network addresses. (*See* Keromytis Decl. ¶ 75); *In re Robertson*, 169 F.3d at 745. For example, X.500 and DNS names for the same server might correspond to the exact same network address. (*See* Keromytis Decl. ¶ 75.) Accordingly, the rejection of claim 26 should be withdrawn. Claim 27 depends from claim 26 so it is patentable for the same reasons as claim 26.

9. Independent Claim 28

Like claim 1, independent claim 28 recites multiple instances of "secure name." This feature is not disclosed in *Lendenmann* for the same reasons discussed above regarding claim 1. And like claim 2, independent claim 28 recites a "secure name service," which *Lendenmann* does not disclose for the same reasons discussed above regarding claim 2. Additionally, as discussed above for claim 2, *Lendenmann* does not disclose a "message requesting a network address" associated with any particular name at all, let alone a "network address associated with a secure name of a device."

Finally, *Lendenmann* also does not disclose the "receiving" or "sending" features of claim 28 for the same reasons discussed above regarding claim 2. Accordingly, the rejection of claim 28 should be withdrawn.

10. Independent Claim 29

Like claim 1, independent claim 29 recites multiple instances of "secure name." This feature is not disclosed in *Lendenmann* for the same reasons discussed above regarding claim 1. And similar to the "receiving" feature of claim 2, independent claim 29 recites "receiving at a network address associated with a secure name of a first device a message." *Lendenmann* does not disclose this feature because *Lendenmann* does not disclose receiving a message at a network address associated with any particular name at all, let alone a "network address associated with a secure name of a first device," as discussed above regarding claim 2. Thus, the rejection of claim 29 should be withdrawn.

For at least these reasons, Patent Owner respectfully requests that the rejection of claims 1-9, 12-15, and 18-29 under § 102(b) based on *Lendenmann* be withdrawn and their patentability confirmed.

G. The Rejection of Claims 10, 11, and 17 Under 35 U.S.C. § 103 Based on *Lendenmann* in View of *Beser* Should Be Withdrawn (Issue 7)

Claims 10, 11, and 17 depend either directly or indirectly from claim 2, so they include all of the features of claim 2. *Lendenmann* does not disclose or suggest the features of claim 2 for the reasons discussed above, and Requester never alleges that *Beser* remedies those deficiencies of *Lendenmann*. (*See* Req. at 160-64, relying on *Beser* only for tunneling features and multimedia features.) Thus, for at least the reasons set forth above, the § 103 rejection of claims 10, 11, and 17 over *Lendenmann* in view of *Beser* should be withdrawn.

H. The Rejection of Claims 10 and 11 Under 35 U.S.C. § 103 Based on *Lendenmann* in View of RFC 2401 Should Be Withdrawn (Issue 8)

Claims 10 and 11 depend from claim 2, and include all of its features. *Lendenmann* does not disclose or suggest the features of claim 2 for the reasons discussed above, and Requester never alleges that RFC 2401 remedies those deficiencies of *Lendenmann*. (*See* Req. at 164-66, relying on RFC 2401 only for tunneling features.) Thus, for at least the reasons set forth above, the § 103 rejection of claims 10 and 11 over *Lendenmann* in view of RFC 2401 should be withdrawn.

I. The Rejection of Claims 1-23 and 28-29 Under 35 U.S.C. § 102(e) Based on *Provino* Should Be Withdrawn (Issue 9)

The Office rejects claims 1-15, 18-23, 28, and 29 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,557,037 to Provino ("*Provino*") (Issue No. 9). (OA at 8-11.) For the reasons discussed below, *Provino* does not disclose each and every feature of the claims, so the rejection should be withdrawn.

1. Overview of *Provino*

Provino discloses a system for connecting an external device to a device on a virtual private network via a secure tunnel between the external device and a firewall associated with the virtual private network. (*Provino* Abstract.) Referring to FIG. 1 of *Provino*, reproduced below, when an operator at a device 12(m) wishes to connect to a device 13 on the Internet, the operator inputs a human-readable address of the device 13, causing the device 12(m) to send a message to a name server 17 requesting the corresponding Internet address of the device 13. (*Id.* at 8:14-40, 11:5-11.) The name server 17 does not have the addresses of the devices 31 on the virtual private network 15, except for the address of the firewall 30 of the virtual private network 15. In response to a request for the Internet address of a device 31 on the virtual private network 15, the name server returns the Internet address of the firewall 30. (*Id.* at 10:45-55, 11:11-16.)

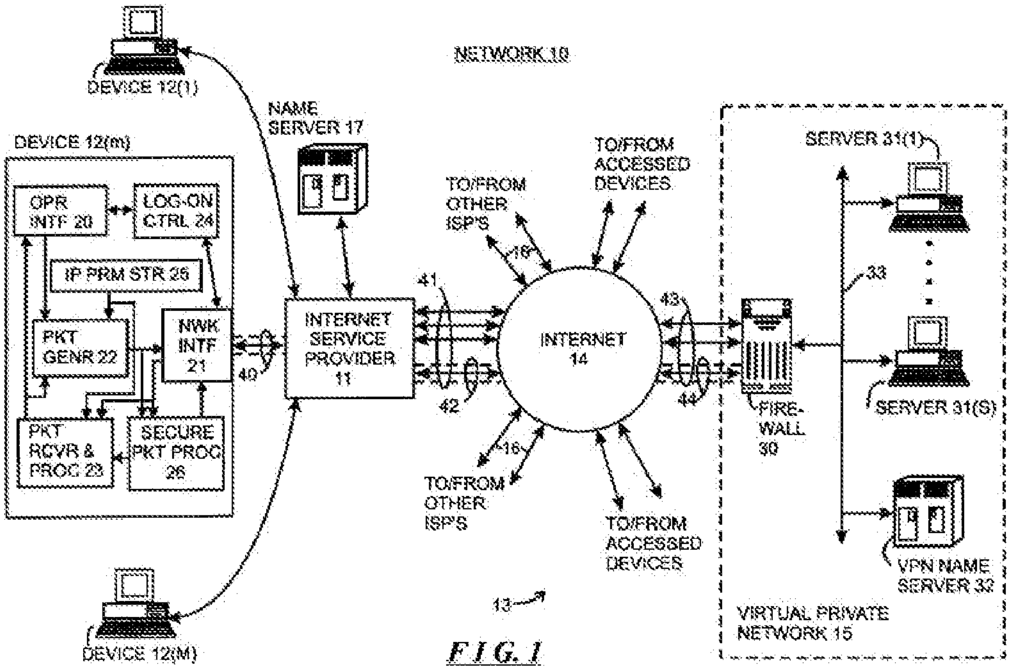


FIG. 1

The device 12(m) initiates establishment of a secure tunnel with the firewall 30. (*Id.* at 9:32-56, 10:56-58, 11:13-16.) Further, the firewall 30 provides the device 12(m) with the identification of a second name server 32 inside the virtual private network 15. (*Id.* at 10:62-63.) The device 12(m) sends, over the secure tunnel, a message to the second name server 32 requesting the Internet address of the device 31 on the virtual private network 31 corresponding to the human-readable address of the device 31. (*Id.* at 10:62-67, 11:17-26.) Thereafter, the device 12(m) is able to communicate with the device 31 on the virtual private network 15 via the secure tunnel.

2. Independent Claim 1

Independent claim 1 recites a number of features that are not taught by *Provino*, as discussed below.

a. *Provino* Does Not Disclose "A First Device Associated with a Secure Name and an Unsecured Name"

Independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." The Office adopts Requester's analysis for this feature (and all other features of claim 1, OA at 8), but Requester's analysis is fundamentally flawed, as *Provino's* system does not function the way Requester alleges. In particular, Requester contends that "Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, *i.e.*, the Domain name stored in the VPN Name Server 32, and one being an unsecured name, *i.e.*, the Domain name stored in Name Server 17 at ISP 11." (Req. at 168.) Requester quotes *Provino* at 10:45-52 to support this allegation, but that passage actually states that name server 17 does not contain *any* name associated with servers 31(S). (Keromytis Decl. ¶ 79.) Instead, "nameserver 17 is not provided with integer Internet addresses for servers 31(S) and other devices which are in the virtual private network 15." (*Provino* 10:48-51.) Thus, "the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(S) which is to be accessed from that nameserver 17." (*Id.* at 10:52-55.) Network addresses related to firewall 30 may be contained in name server 17, but not the network addresses for servers 31(S). (*Id.* at 10:51-52.)

Requester has not identified any device in *Provino* that is associated with both a "secure name" and an "unsecured name." Accordingly, the Requester and the Office have not shown that *Provino* discloses "a non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name." The rejection should be withdrawn.

b. *Provino* Does Not Disclose a "Secure Name"

Claim 1 recites a "secure name" in two places: "a first device associated with a *secure name* and an unsecured name" and "receiving, at a network address corresponding to the *secure name* associated with the first device." *Provino*, however, does not disclose any "secure names." As disclosed and claimed in the '181 patent, "secure names" are those names used to communicate securely that are resolved by a secure name service (*i.e.*, a service that both resolves a name into a network address and further supports establishing a secure communication link). (Keromytis Decl. ¶ 80.) The name servers in *Provino*, on the other hand, are conventional name servers of the type distinguished in the '181 patent specification and do not qualify as a "secure name service" that can resolve "secure names." (*Id.*)

The '181 patent discloses that a conventional domain name service system merely returns an IP address corresponding to a domain name. (*Id.* ¶ 81.) For example, in one embodiment, the '181 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('181 patent 38:54-59; Keromytis Decl. ¶ 81; *see also* '181 patent 38:61-39:13.)

Similar to the conventional domain name systems described by the '181 patent, the name servers 17 and 32 of *Provino* merely return a requested Internet address of a device corresponding to the human-readable address of that device, such as the requested IP address corresponding to a domain name like "Yahoo.com." (*Compare Provino* 8:48-51 *with* '181 patent 38:54-59; *see also* Keromytis Decl. ¶ 82.) In particular, *Provino* discloses that name server 17 "can resolve the human-readable domain names to provide the appropriate Internet address for the destination referred to in the respective human-readable name." (*Provino* 7:40-43.) It resolves names for devices located outside the firewall 30 and for the name of the firewall itself. (Keromytis Decl. ¶ 82.) Name server 32 operates in a similar manner except it resolves addresses for servers 31(s) behind firewall 30. (*Provino* 9:2-5, stating that name server 32 merely "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses"; Keromytis Decl. ¶ 82.) In both instances, name servers 17 and 32 operate in the conventional manner described and distinguished in the '181 patent specification in that they merely resolve a requested human-readable address but do not resolve "secure names" or support establishing a secure communication link as in the case of a secure name service.

The '181 patent recognizes that such conventional domain name systems suffer from certain drawbacks and thus discloses embodiments that address them, including embodiments with secure name services that resolve "secure names" as recited in claim 1. (*See, e.g.*, '181 patent 39:23-25; Keromytis Decl. ¶ 82.) Since *Provino*'s alleged name services (*i.e.*, name servers 17 and 32) are merely conventional domain name servers of the type distinguished by the '181 patent, the alleged domain names stored in the conventional domain name servers of *Provino* cannot correspond to a "secure name," as recited in claim 1.

c. *Provino* Does Not Disclose the Claimed "First Device"

Because the claims require that the "first device" be "associated with a secure name and an unsecured name," *Provino* does not disclose the claimed "first device" for the reasons discussed above in Sections (I)(2)(a) and (b). Accordingly, *Provino* does not disclose the following features, which also require the undisclosed "first device":

- receiving, at a network address corresponding to the secure name associated with the *first device*, a message from a second device of the desired to securely communicate with the *first device*; and
- sending a message over a secure communication link from the *first device* to the second device.

Requester implicitly recognizes that no "first device" exists having all of the claimed features, as it mixes and matches features from different devices in its attempt to show unpatentability. In particular, Requester initially contends that each server 31(S) behind firewall 30 qualifies as the "first device" allegedly having secure and unsecured names associated with it. (Req. at 168, "Provino additionally discloses two names associated for each of the servers (items 31(S), for example) . . . one being a secure name . . . and one being an unsecured name.") But when later attempting to establish the "receiving" feature of claim 1, Requester contends that device 12(m) located outside of firewall 30 is the claimed "first device." (Req. at 171, "the secure communication link between devices can be initiated by a first device (device 12(m)) . . . .") That Requester has resorted to this sleight of hand, indiscriminately referring to multiple devices that have different features as though they were the one and the same device, confirms that the claimed "first device" is not disclosed in *Provino* as arranged in the claims, so the rejection should be withdrawn. *See Net MoneyIn, Inc.*, 545 F.3d at 1369 ("unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it . . . cannot anticipate under 35 U.S.C. § 102.").

d. *Provino* Does Not Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desired to Securely Communicate with the First Device"

Requester provides virtually no analysis to demonstrate how *Provino* allegedly discloses the claimed "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." The entirety of the analysis consists of quoting the claim language and alleging the following, which relies on device 12(m) as being the "first device" associated with both secure and unsecured names:

> Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12 (m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52.

(Req. at 171.)

Requester's brief argument is flawed because device 12(m) is not associated with a secure name. Indeed, Requester never alleges that it is, instead contending only that server 31(S) is associated with a secure name. (*See* Req. at 168.) Thus, device 12(m) cannot receive anything "at a network address corresponding to the secure name associated with the first device" because it has no secure name associated with it in the first place. (Keromytis Decl. ¶ 85.)

Requester's argument is also flawed because, if one were to assume that server 31(S) had an associated secure address as alleged by Requester—a premise that is false for the reasons discussed above, Requester's allegations would still not demonstrate the claimed "receiving." As Requester acknowledges, it is the *firewall 30* that receives messages from device 12(m) to create a tunnel, not server 31(S). In fact, server 31(S) does not receive the alleged request "requesting establishment of a secure tunnel between the device 12(m) and firewall 30," and Requester never contends that it does. (*See* Req. at 171; *see also* Keromytis Decl. ¶ 86.) Consequently, Requester has failed to identify any device that receives, "at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device."

3. Independent Claim 2

Similar to claim 1, independent claim 2 recites a device having a "secure name." For the reasons discussed above in Section III.I.2.b, this feature is not disclosed in *Provino*. Claim 2 also recites a "secure name service," but since name servers 17 and 32 are both conventional name servers of the type distinguished by the '181 patent, they are not the claimed "secure name service." (*See supra* Section III.I.2.b.)

4. Dependent Claims 3-15 and 18-22

Claims 3-15 and 18-22 depend directly or indirectly from claim 2 and include all of its features. They are patentable for at least the reasons discussed above regarding claim 2.

5. Dependent Claim 23

Claim 23 depends from claim 2 and is patentable for at least the reasons discussed above regarding that claim. Claim 23 also recites that "the secure name of the second device is a secure, non-standard domain name." As explained above, *Provino* discloses only conventional domain-name functions and only resolves conventional domain names. Accordingly, *Provino* does not disclose the claimed "non-standard domain name."

6. Independent Claim 28

Like claim 1, independent claim 28 recites multiple instances of "secure name." This feature is not disclosed in *Provino* for the same reasons discussed above regarding claim 1. And like claim 2, claim 28 further recites a "secure name service." This feature is not disclosed in *Provino* for the same reasons discussed above regarding claim 2.

7. Independent Claim 29

Independent claim 29 recites multiple instances of "secure name." This feature is not disclosed in *Provino* for the same reasons discussed above regarding claim 1. Claim 29 also recites "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." Accordingly, it is not disclosed in *Provino* for the same reasons discussed above regarding the similar feature of claim 1.

In view of the above, the § 102(e) rejections of claims 1-15, 18-23, 28, and 29 based on *Provino* should be withdrawn.

J. The Obviousness Rejections Based on *Provino* and *H.323* Should Be Withdrawn (Issue 10)

The Office rejected claims 24-26 under 35 U.S.C. § 103 as being obvious over *Provino* in view of "H.323 Packet-based Multimedia Communications Systems" ("*H.323*") (Issue No. 10). (OA at 11.) For the reasons discussed below, the combination of *Provino* and *H.323* does not disclose each and every feature of the claims, so the rejection should be withdrawn.

1. Independent Claim 24 and Dependent Claim 25

Requester's proposed rejections based on *Provino* and *H.323*, which the Office adopted wholesale (OA at 11), are deficient in several ways. For example, as explained regarding claim 1, *Provino* does not disclose any "secure names" because there is no secure name service to resolve secure names. To the extent the Office contends that *H.323* discloses secure names, this position is incorrect for the reasons discussed in more detail below in the *H.323* anticipation section. (*See* Section III.K.3.) Thus, the proposed combination does not teach the claimed "secure name" recited in several places in independent claim 24 and dependent claim 25.

Claim 24 (and claim 25, by virtue of its dependence on claim 24) also recites "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." It is not disclosed in *Provino* for the same reasons discussed above regarding the similar feature of claim 1. If the Office contends that *H.323* discloses this feature, this position is incorrect for the reasons discussed in more detail below in the *H.323* anticipation section, Section III.K.3.

2. Independent Claim 26

Although styled as a rejection based solely on *Provino* and *H.323*, Requester and the Office also rely on "H.235 Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals" ("*H.235*") in attempting to establish unpatentability for claim 26. (OA at 11, adopting Requester's analysis; Req. at 199-200, quoting H.235.) *H.235*, however, is not incorporated by reference into *H.323* and is therefore not properly considered to be part of that document. Section III.K.1 below provides additional details on why it is legally and factually improper to include it in the rejection as though it were incorporated by reference into *H.323*. For now, it is sufficient to note that the Requester's proposed rejection is both legally and procedurally deficient and can be withdrawn on that basis alone.

The rejection is also substantively deficient. Requester relies on *Provino* for its alleged disclosure of secure names, among other things, and primarily relies on *H.323* for its alleged disclosure of a name registration mechanism. This combination does not teach many claimed features.

For example, similar to claim 1, independent claim 26 recites that a first device must be associated with both an unsecured name and a secure name. In particular, claim 26 recites "obtaining registration of an *unsecured* name associated with the first device." It also recites "obtaining registration of a *secure* name associated with the first device." As explained for claim 1, Requester and the Office have not identified any device in *Provino* that has both secure and unsecured names. As also explained regarding claim 1, *Provino* does not disclose any "secure names" in the first place because there is no secure name service to resolve those secure names. To the extent the Office contends that *H.323* discloses secure and unsecured names, this position is incorrect for the reasons discussed in more detail below in the *H.323* anticipation section, Section III.K.3.

Claim 26 also recites "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." It is not disclosed in *Provino* for the same reasons discussed above regarding the similar feature of claim 1. To the extent the Office contends that *H.323* discloses this feature, this position is incorrect for the reasons discussed in more detail below in the *H.323* anticipation section, Section III.K.3.

In view of the above, the § 103 rejections of claims 24-26 based on *Provino* and *H.323* should be withdrawn.

K. The Rejection of Claims 1-29 Under 35 U.S.C. § 102(b) Based on *H.323* Should Be Withdrawn (Issue 11)

1. Combining the Teachings of *H.323, H.245, H.235,* and *H.225* Is Improper

Claims 1-29 are rejected under 35 U.S.C. § 102(b) over the reference "H.323 Packet-based Multimedia Communications Systems" ("*H.323*").[4] The Office and Requester contend that *H.323* expressly incorporates the reference "H.225.0 Call Signalling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems" ("*H.225*"), the reference

[4] The Office Action states that "Claims 1-9 and 12-29 are rejected under 35 U.S.C. 102(b) as being obvious over H.323." (Office Action at 11.) In view of the § 102(b) rejection, Patent Owner submits that this statement appears to be a typographical error, and that the Office Action meant to state that claims 1-9 and 12-29 are rejected under 35 U.S.C. 102(b) as being *anticipated by* H.323. Indeed, the Request originally proposed under Ground No. 12 that claims 1-29 are rendered obvious in view of *H.323* in conjunction with *H.225*, *H.235*, and *H.245* under 35 U.S.C. § 103, but the Office Action did not adopt this rejection. Indeed, the Order Granting/Denying Request for *Inter Partes* Reexamination stated that Ground No. 12 proposed by the Request does not establish that there is a reasonable likelihood that the Requester will prevail with respect to claims 1-29. (Order Granting/Denying Request for *Inter Partes* Reexamination at 19.)

Nevertheless, assuming *arguendo* the statement in the Office Action is not a typographical error, a rejection that leaves an applicant guessing as to the basis of the rejection is improper. *Ex parte Schricker*, 56 USPQ2d 1723, 1725 (B.P.A.I. 2000) (unpublished) (remanding when an examiner left an applicant and the board to guess as to whether a rejection is based on § 102 or § 103). Since the rejection of claims 1-29 based on *H.323* refers to elements of both § 102 and § 103, Patent Owner is left guessing as to the basis of the rejection. Accordingly, Patent Owner respectfully submits that such a rejection is improper, and reconsideration and withdrawal of the rejection of claims 1-29 based on *H.323* are respectfully requested. Should the Office Action decide to maintain the rejection of claims 1-29 based on *H.323*, clarification of the rejection, together with a new Office Action, are respectfully requested.

"H.235 Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals" ("*H.235*"), and the reference "H.245 Control Protocol for Multimedia Communication" ("*H.245*"). (Req. at 204.) The Request states that *H.225*, *H.235*, and *H.245*, are "incorporated by reference because they are specifically referenced and described as disclosing particular features of the H.323 recommendation." (*Id.*) This is incorrect.

To incorporate matter by reference, a host document must contain language "clearly identifying the subject matter which is incorporated and where it is to be found." *In re de Seversky*, 474 F.2d 671, 674 (CCPA 1973). A "mere reference to another application, or patent, or publication is not an incorporation of anything therein." *Id.* Put differently, "the host document must *identify with detailed particularity* what specific material it incorporates and *clearly indicate* where that material is found in the various documents." *Adv. Display Sys., Inc.*, 212 F.3d at 1282 (emphasis added).

H.323 does not identify with detailed particularity the subject matter of *H.225*, *H.235*, and *H.245* allegedly incorporated. Nor does *H.323* clearly indicate where that material is found in the references. For example, the Office Action and Request rely on *H.235* as teaching a variety of features that, when combined with *H.323*, allegedly disclose the claimed features of the '181 patent. (Req. at 214-217, 219-231, 235-236, 245-247, 254-256, and 259-269.) But *H.323* generically states: "Authentication and security for H.323 systems is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235." (*H.323* 81.) Thus, *H.235* is not incorporated into *H.323*, as *H.323* fails to identify "with detailed particularity" the subject matter incorporated and where it can be found. *In re de Seversky*, 474 F.2d at 674; *Adv. Display Sys., Inc.*, 212 F.3d at 1282.

Similarly, the Office and Requester rely on *H.225* as allegedly teaching names of gatekeepers registered in a DNS, multiplexing points, and endpoint registration. (Req. at 210, 211, 233, 238, 239, 251, and 269.) But *H.323* does not identify with any particularity which portions of *H.225* are allegedly incorporated. Nor does *H.323* clearly indicate where these portions are located in *H.225*. Thus, *H.225* is not incorporated by reference. *In re de Seversky*, 474 F.2d at 674; *Adv. Display Sys., Inc.*, 212 F.3d at 1282.

The Request does not actually cite to *H.245*, and has not made clear the specific material of *H.245* that it relies on in this rejection. Thus, *H.323* has not been shown to identify with detailed particularity what specific material of *H.245* is incorporated, nor has *H.323* been shown to clearly indicate where that material is found in *H.245*.

Because this attempt to incorporate by reference *H.225*, *H.235*, and *H.245* into *H.323* is improper, the Office relies on multiple references in forming its § 102 rejections. But "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in *a single prior art reference*." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987) (emphasis added). As the Federal Circuit has stated, it is "clear that anticipation does not permit an additional reference to supply a missing claim limitation." *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1335 (Fed. Cir. 2002). Because the § 102 rejection of claims 1-29 based on *H.323* relies on many such additional references to supplement *H.323*, the rejection is improper and should be withdrawn.

Nevertheless, even if one improperly assumes that *H.225*, *H.235*, and *H.245* are incorporated into *H.323*, either as to certain sections or in their entirety, claims 1-29 are patentable over *H.323*, *H.225*, *H.235*, and *H.245* (collectively referred to as "the combined *H.323* references") for at least the reasons discussed below.

2. Overview of *H.323*

H.323 describes the components of an H.323 system, which provides multimedia communications services over Packet Based Networks (PBN). (*H.323* i.) Various remote endpoints may communicate over the H.323 system via point-to-point calling. (*Id.* at 4-5, "3.7 call.") Endpoints may include a terminal, a gateway, or a multipoint control unit (MCU). (*Id.* at 5, "3.14 endpoint.") Other non-callable entities include gatekeepers and multipoint conferences. (*Id.*, "3.9 callable.") *H.323* explains that each entity has at least one network address, and that endpoints may additionally be associated with one or more alias addresses. (*Id.* at 33.) An alias address may represent either an endpoint itself or a service (*e.g.*, a conference) hosted by an endpoint. (*Id.*) An access token may shield an endpoint's alias address and transport address (*i.e.*, network address plus a TSAP identifier) from another endpoint during the calling process. (*Id.* at 38; *id.* at 8, "3.42 transport address.")

When establishing a call, one endpoint may call another via a gatekeeper. (*Id.* at 34.) Endpoints must register with a gatekeeper in order to participate in gatekeeper functions. (*Id.* at 37.) For example, gatekeepers may translate alias addresses to transport addresses, although any potential directory services are undefined. (*Id.* at 27.) Other functions include admissions control, bandwidth control, and zone management, among others. (*Id.* at 33.) Using access tokens requires endpoints to route communications through a gatekeeper. (*Id.* at 38.) Endpoints may also call each other directly, particularly when no gatekeeper exists in an H.323 system. (*See, e.g., id.* at 27.)

Establishing a call proceeds through the process of "call signalling." (*Id.* at 33.) The call procedures occur as follows: (A) call setup, (B) initial communication and capability exchange, (C) establishment of audiovisual communication, (D) call services, and (E) call termination. (*Id.* at 41.)

3. Independent Claim 1

a. The Combined *H.323* References Do Not Disclose "a First Device Associated with a Secure Name and an Unsecured Name"

Independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." The combined *H.323* references do not disclose these claim features.

The Office and Requester assert that alias addresses protected by "access tokens" correspond to secure names. (OA at 11; Req. at 209.) They also assert that an endpoint having an access-token-protected alias (*i.e.*, an alleged "first device") could additionally have an alias corresponding to an "unsecured name." (OA at 11; Req. at 210-11.) The Office and Requester also allege that a uniform resource locator (URL) for a gatekeeper corresponds to the "unsecured name." (OA at 11; Req. at 210-11.) They further assert that if the endpoint having an access-token-protected alias is a gateway, a first Switched Circuit Network (SCN) endpoint obtaining access to the PBN via the gateway might have an alleged "unsecured name," and that a second SCN endpoint obtaining access to the PBN via the gateway might have a "secure name." (Req. at 212-13.) This is incorrect.

The Office and Requester's allegation that the URL for a gatekeeper corresponds to the unsecured name recited in independent claim 1 is incorrect. (Keromytis Decl. ¶ 92.) *H.225* discloses that the URL is for the gatekeeper. (*H.225* 141.) Thus, the URL (*e.g.*, the alleged unsecure name) is associated with the gatekeeper rather than the called *H.323* endpoint (*e.g.*, the alleged first device). (*Id.*; Keromytis Decl. ¶ 92.) Thus, the URL for the gatekeeper cannot correspond to the unsecured name, because independent claim 1 recites that the unsecured name is associated with the first device.

The Office and Requester also allege that if the *H.323* endpoint is a Gateway, (*see* Req. at 211), a first SCN endpoint that is obtaining access to the PBN through the Gateway has an unsecure name. (Req. at 212-13.) This is also incorrect. (Keromytis Decl. ¶ 93.) The first SCN endpoint that is allegedly obtaining access to the PBN through the Gateway does not have an unsecure name. (*Id.*) The Office and Requester point to pages 4-6 of *H.323* as support for this allegation. (Req. at 212-13.) However, nowhere in these cited portions does *H.323* mention any name for the first SCN endpoint, let alone an unsecure name. The cited portions simply state that "[i]n case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway." (*H.323* 4-5.)

Moreover, since the Office and Requester allege that the first SCN endpoint has the alleged unsecure name, this alleged unsecure name is associated with the first SCN endpoint rather than with the Gateway (*e.g.*, the alleged first device). (*Id.*) Accordingly, the alleged unsecure name of the first SCN endpoint cannot correspond to the unsecure name recited in independent claim 1.

Furthermore, nowhere do the *H.323* references disclose that when an access token is used to protect an alias address of a called endpoint (*i.e.*, the alleged secure name), the called endpoint would also have a different alias address that is not protected by the access token (*i.e.*, the alleged unsecure name). (Keromytis Decl. ¶ 94.) Indeed, the Office and Requester fail to show a single embodiment in the combined *H.323* references in which the called endpoint has an alias address protected by an access token (*i.e.*, an alleged secure name) as well as another alias address not protected by an access token (*i.e.*, an alleged unsecured name). The mere generic assertion that "a single endpoint may have multiple aliases" does not and cannot make the further leap of disclosing that endpoints may have both access tokens and additional aliases, and that such features are "secure" and "unsecured" names. (*See* Req. at 210.) Simple repetition of this argument does not make it true. (*See, e.g.*, *id.* at 211, merely specifying that "MCUs and Gateways are endpoints and register multiple Alias names.")

Furthermore, Requester has not shown how an alias address protected by an access token or the access token itself corresponds to the "secure name" recited in claim 1. (Keromytis Decl. ¶ 95.) The Office and Requester point to page 38 of *H.323* as allegedly disclosing the secure name recited in independent claim 1. However, nowhere does this cited portion disclose the term "secure," let alone disclose the term "secure name." (*See H.323* 38.) While this cited portion states that access tokens "provide privacy by shielding an endpoint's Transport Address and Alias address information from a calling party", providing privacy for an alias address would not render such an alias address to be a secure name as recited in independent claim 1. (*H.323* 38; Keromytis Decl. ¶ 95.) Moreover, to the extent Requester alleges that an access token itself may correspond to a "secure name," the two-word parenthetical in which this allegation appears to be made fails to provide any shred of support or explanation, and the § 102(b) rejection should be withdrawn. *Net MoneyIN*, 545 F.3d at 1369 ("the proponent must show 'that the four corners of a single, prior art document describe every element of the claimed invention.'"). Finally, the second SCN endpoint cannot correspond to the "secure name" for at least similar reasons as discussed with respect to the first SCN endpoint. (Keromytis Decl. ¶ 96.)

Accordingly, the combined *H.323* references fail to disclose "a first device associated with a secure name and an unsecured name," and the rejection should be withdrawn.

b. The Combined *H.323* References Do Not Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desired to Securely Communicate with the First Device"

Independent claim 1 recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." The combined *H.323* references do not disclose these claim features.

As discussed above, the Office and Requester assert that an alias address protected by an access token or the access token itself corresponds to the "secure name" recited in claim 1. (*See* Req. at 214.) But *H.323* does not describe receiving any message at a network address corresponding to an access-token-protected alias *rather than* a second, allegedly "unsecured" alias. Nor does the Request assert that it does. (*See* Req. at 213-14.) Furthermore, *H.323* discloses that its access tokens merely "shield[] an endpoint's Transport Address and Alias Address," and therefore *H.323* does not disclose any "message . . . of the desired to securely communicate." (*H.323* 38; Keromytis Decl. ¶ 98.) As explained above with respect to *Beser*, merely shielding the endpoints of communications does "not <u>secure</u> those communications from eavesdropping." (*Supra* Section III.B.2.c.ii.) And therefore, any access-token-related messages do not communicate a "desire[] to securely communicate," as recited in claim 1. Thus, the rejection is improper and should be withdrawn.

To remedy *H.323*'s shortcomings, Requester improperly attempts to import *H.235* passages into *H.323*. (Req. at 214.) The Requester views *H.323* as inviting wholesale incorporation of *H.235* by reference, which is improper for the reasons discussed above. *Adv. Display Sys., Inc.*, 212 F.3d at 1282 ("[T]he host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents.")

But regardless of whether *H.235* is incorporated into *H.323*, it nevertheless fails to disclose receiving any "message . . . of the desire[] to securely communicate" at a network address corresponding to any access-token-protected alias address (*i.e.*, alleged secure name). Without identifying any message in particular, the Requester points to at least five sections of *H.235* as disclosing these features. But despite citing these different passages, Requester fails to point out any single message in support of its arguments. The rejection should be withdrawn for this reason. *See In re Spada*, 911 F.2d 705, 709, 15 USPQ2d 1655 (Fed. Cir. 1990); *In re King*, 801 F.2d 1324, 231 USPQ 136 (Fed. Cir. 1986); *In re Jung*, 637 F.3d 1356, 1362 (Fed. Cir. 2011); *Chester*, 906 F.2d

1574, 1578 (Fed. Cir. 1990); *Ex parte Schricker*, 56 USPQ2d at 1725. But even if one improperly assumes that the rejection had a basis, each section fails to support the rejection.

First, the *H.235* token feature does not disclose the "message" features recited in claim 1. (*See* Req. at 214-15.) Any messages associated with the *H.235* token feature serve merely to "obscure or hide destination addressing information," not to communicate any desire to securely communicate. (*H.235* 28-29.) Indeed, as discussed above, obscuring or hiding the endpoints of communications "does not *secure* those communications from eavesdropping," and therefore any security-token-related messages do not communicate a desire to securely communicate. (*See* Keromytis Decl. ¶ 100.)

Second, the IPsec passage of *H.235* also fails to support the rejection. (*See* Req. at 215-16.) The only address disclosed in this passage corresponds to a "call signalling channel," not to an endpoint (*i.e.*, an alleged "first device"). (Keromytis Decl. ¶ 101.) Thus, the IPsec passage cannot disclose any network address corresponding to a secure name, as recited in claim 1. *H.235* also does not explain any relationship or interaction between IPsec and an access token or an access-token-protected alias addresses (*i.e.*, alleged "secure" names), much less how IPsec negotiations would proceed between one or more devices employing such tokens. (*H.235* 30-31; Keromytis Decl. ¶ 102.) Nor does the Requester assert that it does. (*See* Req. at 215-16.) Furthermore, *H.235* does not disclose whether or how the H.245 channels utilized by IPsec may implement its features through a gatekeeper-routed connection, which is required when access tokens are employed. (*H.323* 38; *H.235* 30, disclosing no gatekeeper functions when a call is established, and disclosing no gatekeeper role at all beyond step 1; Keromytis Decl. ¶ 102.) Thus, the *H.235* IPsec feature does not disclose the features of claim 1.

Third, the "Call establishment security" feature of *H.235* additionally fails to support the rejection. (*See* Req. at 216.) The "connection messages" disclosed in this *H.235* passage occur only *after* security features have already been employed, and therefore these messages cannot correspond to a "message . . . of the desired to securely communicate," as recited in claim 1. (*H.235* 6, "a secure mode of communication should be used . . . *before* the exchange of call connection messages," emphasis added; Keromytis Decl. ¶ 103.) Moreover, a "call establishment channel" is an entirely undefined term, and is nowhere described as a channel between the endpoints alleged to correspond to the "first device" and "second device" of claim 1. (*See generally H.235*, *H.323* 4-8.) *H.235* also discloses no relationship or interaction between call establishment security and an access token or access-token-protected alias address (*i.e.*, alleged "secure" name), let alone how call establishment security would proceed with one or more devices employing such tokens. Thus, the "Call establishment security" feature of *H.235* does not disclose the features of claim 1.

Fourth and fifth, the "Call control (H.245) security" and "Media stream privacy" passages of *H.235* also fail to support the rejection. (*See* Req. at 216-17.) These passages do not describe receiving any message at a network address corresponding to an access token or an access-token-protected alias address (*i.e.*, an alleged secure name). (*H.235* 6-7; Keromytis Decl. ¶ 104.) Nor does the Request assert that they do. (*See* Req. at 216-17.) *H.235* also does not disclose whether or how the necessary H.245 channels may implement the alleged security features through a gatekeeper-routed connection, which is required when access tokens are employed. (*H.235* 6-7; *H.323* 38; Keromytis Decl. ¶ 104.) Instead, *H.235* merely teaches that implementation of the security features in these passages lies within the discretion of the calling endpoint. (*Id.* at 6-7, "The H.245 channel shall be secured using any negotiated privacy mechanism (*this includes the option of 'none'*)," "any participating endpoints *may* utilize an encrypted H.245 channel"; Keromytis Decl. ¶ 104.) Thus, these *H.235* passages fail to disclose the features of claim 1.

For all of the above reasons, *H.323* fails to disclose "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." And the various passages of *H.235* do not remedy *H.323*'s shortcomings, even if one improperly assumes that they could be incorporated by reference. *Adv. Display Sys., Inc.*, 212 F.3d at 1282. The rejection of claim 1 should be withdrawn, and its patentability confirmed.

c. The Combined *H.323* References Do Not Disclose "Sending a Message over a Secure Communication Link from the First Device to the Second Device"

The Office and Requester do not identify any message at all corresponding to a message sent "from the first device to the second device," instead generically asserting that "[t]he result of step (a) above is sending a message . . . from the first device to the second device." (OA at 11; Req. at 217.) This fails to support the rejection. *See In re Spada*, 911 F.2d at 709, 15; *In re King*, 801 F.2d at 1324; *In re Jung*, 637 F.3d at 1362; *Chester*, 906 F.2d at 1578; *Ex parte Schricker*, 56 USPQ2d at 1725; *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d at 1369 ("the proponent must show 'that the four corners of a single, prior art document describe every element of the claimed invention.'") (internal citations omitted).

Moreover, the Request has failed to establish that any of the passages in the combined *H.323* references disclose a "secure communication link." As discussed above, a reference must disclose *data security* (*i.e.*, encryption) in order to disclose a "secure communication link." Otherwise, the reference's purported secure communication link "will not *secure* those communications from eavesdropping." (Keromytis Decl. ¶ 105.) Here, the access token section of *H.323* does not disclose encrypted communications between endpoints. (*H.323* 38.) Neither do the security token passages of *H.235*, because they merely disclose encryption of the tokens themselves. (*H.235* 28-29.) Neither does the "Call establishment security" passage of *H.235*. (*Id.* at 6.) *H.235* additionally fails to disclose whether or how the IPsec, "Call control (H.245) security" and "Media stream privacy" features utilizing H.245 channels are implemented in conjunction with access-token-protected aliases, or are implemented through gatekeeper-routed connections, which are required when access tokens are employed. (*H.235* 6-7, 30-31; *H.323* 38; Keromytis Decl. ¶ 105.) Thus, the rejection of claim 1 should be withdrawn, and its patentability confirmed.

4. Independent Claim 2

The combined *H.323* references do not disclose at least the following features of claim 2.

a. The Combined *H.323* References Do Not Disclose "a Secure Name"

The Office and Requester allege that an alias address of a called endpoint protected by an access token corresponds to the secure name recited in independent claim 2. (Req. at 220.) This is incorrect for at least similar reasons as discussed above with respect to independent claim 1. (*Id.*)

b. The Combined *H.323* References Do Not Disclose "a Network Address Associated with the Secure Name of the Second Device"

The Office and Requester fail to identify with any specificity what teaching in the combined *H.323* references corresponds to the "network address associated with the secure name of the second device," as recited in claim 2. Requester cites to many different passages, but fails to identify even one specific address in support of its arguments. Thus, the rejection should be withdrawn. *See In re Spada*, 911 F.2d at 709, 15; *In re King*, 801 F.2d at 1324; *In re Jung*, 637 F.3d at 1362; *Chester*, 906 F.2d at 1578; *Ex parte Schricker*, 56 USPQ2d at 1725.

To the extent Requester alleges that the address mentioned in the IPsec passage of *H.235* corresponds to the "network address" of claim 2, this is also incorrect. This address corresponds to "the call signalling channel" rather than the called endpoint (*i.e.*, the alleged "second device"). (*H.235* 30-31; *see also H.323* 5, defining these components.) Thus, Requester has failed to demonstrate that the IPsec and security token passages of *H.235* disclose a "network address associated with the secure name of the second device," as recited in claim 2.

Accordingly, the rejection should be withdrawn, as the combined *H.323* references have not been shown to disclose even a single specific address corresponding to "a network address associated with the secure name of the second device," as recited in claim 2.

c. The Combined *H.323* References Do Not Disclose "from the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated with the Secure Name of the Second Device" and "at the First Device, Receiving a Message Containing the Network Address Associated with the Secure Name of the Second Device"

The combined *H.323* references do not disclose these claim features. The Office and Requester assert that an alias address protected by an access token corresponds to a "secure name." (OA at 11; Req. at 220.) But even if one incorrectly assumes this to be true, using access tokens in *H.323* necessarily prevents the calling endpoint (*i.e.*, the alleged "first device") from ever receiving a network address. (*H.323* 38; Keromytis Decl. ¶ 108.) Indeed, *H.323* specifies that access tokens "provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party." (*H.323* 38.) An access token requires routing communications through a gatekeeper because the "[g]atekeeper will know the endpoint related to the Access Token," unlike the calling endpoint. (*Id.*) Indeed, *H.323* states "A user may give out *only* the Access Token for a calling party to use in reaching the endpoint." (*Id.*) Thus, because a calling endpoint using an access token never receives a network address associated with the access-token-protected alias address, *H.323* does not disclose "receiving a message containing the network address associated with the secure name of the second device," as recited in claim 2. (Keromytis Decl. ¶ 108.)

Requester additionally relies on the security token passage of *H.235* as disclosing the "sending a message to a secure name service" and "receiving a message containing the network address" features of claim 2. (Req. at 218-23.) But even if one incorrectly assumed that *H.235* could be incorporated by reference into *H.323*, the *H.235* security token feature does not utilize an alias address protected by an access token. (*H.235* 28-29; Keromytis Decl. ¶ 109.) Accordingly, it does not disclose "sending a message . . . requesting a network address *associated with the secure name* of the second device," and "receiving a message containing the network address *associated with the secure name*."

Indeed, the Office and Requester cannot point to the use of security tokens in *H.235* as providing an example of using access tokens. Nowhere does *H.323* or *H.235* disclose that an access token is the same as a security token. Furthermore, in the security token embodiment, the Office and

Requester allege that the POTS-B corresponds to the second device recited in independent claim 2. (Req. at 220-23.) However, the POTS-B is not the same as the called endpoint, which the Office and Requester previously alleged as corresponding to the second device recited in independent claim 2. (*Id.* at 219-20 and 223-26.) While the called endpoint is disclosed as providing multimedia communications services over a packet based network (PBN), the POTS-B provides communications over a switched circuit network (SCN). (*H.323* 2; *H.235* 28.) Because the Office and Requester are mixing different embodiments from *H.323* and *H.235* as corresponding to the second device recited in independent claim 2, the Office and Requester have failed to show how the combined *H.323* references disclose all the elements of independent claim 2 as arranged in this claim. *See Net MoneyIN Inc.*, 88 USPQ2d at 1758. Thus, the *H.235* security token feature does not involve any allegedly secure name (*i.e.*, an access-token-protected alias address), and thus does not support the rejection.

Moreover, the Office and Requester fail to identify with any specificity what teaching in the combined *H.323* references corresponds to the "message requesting a network address" or the "message containing the network address" recited in claim 2. Requester cites to many different passages, but fails to point out any message in support of its arguments. Thus, the rejection should be withdrawn. *See In re Spada*, 911 F.2d at 709, 15; *In re King*, 801 F.2d at 1324; *In re Jung*, 637 F.3d at 1362; *Chester*, 906 F.2d at 1578; *Ex parte Schricker*, 56 USPQ2d at 1725.

Requester further relies on the IPsec passage of *H.235* as supporting the rejection in various ways, asserting that "H.323 secures the name of an Alias address via IPSec when the calling endpoint queries the Gatekeeper." (Req. at 221-22.) But the IPsec passage itself explains that "the gatekeeper will inform the endpoint of the address and port number of the call signalling channel" over a pre-existing secure RAS channel. (*H.235* 30, step 1; Keromytis Decl. ¶ 110.) Thus, *H.235* explains that the *RAS channel is secure*—not that any name allegedly provided to the gatekeeper is secure. (*H.235* 30, step 1.) Furthermore, the address provided by the gatekeeper corresponds to a "call signalling channel," not a called endpoint, and therefore does not correspond to the network address associated with the secure name of the alleged "second device." (*Id.*) Accordingly, the IPsec passage does not disclose at least the "secure name," the "sending a message . . . requesting a *network address associated with the secure name of the second device*," and the "receiving a message containing the *network address associated with the secure name of the second device*" features of claim 2.

Additionally, by invoking the IPsec passage here, the Request attempts to rely on a different feature as corresponding the "secure name" of claim 2 than the feature used to correspond to the "secure name" of claim 1 (*i.e.*, an access-token-protected alias address). The Request also fails to explain how this newly alleged "secure name" would be implemented to disclose each and every additional element of claim 2. Thus, this improper mixing and matching of various features from the various combined *H.323* references fails to support the rejection, and the patentability of claim 2 should be confirmed. *Net MoneyIN*, 545 F.3d at 1369.

d. The Combined *H.323* References Do Not Disclose a "From the First Device, Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

Independent claim 2 recites, among other things, "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." For similar reasons discussed above with respect to claim 1, the "Call establishment security," "Call control (H.245) security, and "Media stream privacy" features of *H.235* all fail to disclose a "secure communication link.

Requester additionally relies on the IPsec passage of *H.235* to disclose the foregoing features recited in claim 2, which it did not do with respect to claim 1. But although *H.235* discloses a gatekeeper participating in returning an address and port number to the calling endpoint, (*H.235* at 30, step 1), it does not disclose whether or how encryption would be employed over a gatekeeper-routed H.245 channel, which is required when access-token-protected alias addresses (*i.e.*, alleged "secure" names) are employed. (*Id.* at 30-31; *H.323* 38; Keromytis Decl. ¶ 112.) Instead, *H.235* explains that person-to-person Q&A authentication measures may occur, which is inconsistent with a gatekeeper-routed connection. (*H.235* 30; Keromytis Decl. ¶ 112.) *H.235* also explains that routing H.245 channels through various intermediate devices, including *proxies* and firewalls, is incompatible with employing encryption on those channels. (*H.235* 31; Keromytis Decl. ¶ 112.) And finally, the only address disclosed with respect to the IPsec passage corresponds to a "call signalling channel," not the alleged "second device" (*i.e.*, a called endpoint) of claim 2. (*H.235* 30.) Thus, the IPsec passage of *H.235*, even if one incorrectly assumed that it could be incorporated into *H.323*, fails to disclose a "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link," as recited in claim 2.

Thus, for the above reasons, the rejection of claim 2 should be withdrawn, and its patentability confirmed.

e. Dependent Claims 3-23

Claims 3-23 depend directly or indirectly from claim 2. Accordingly, these claims are patentable for at least the reasons discussed above with respect to claim 2. Furthermore, the § 102(b) rejection of claims 4, 5, 9-11, 13, and 21 should be withdrawn for the additional reasons set forth below.

f. Dependent Claim 4

Having identified an alias address protected by an access token as corresponding to the "secure name" recited in claims 1 and 2, (*see* Req. at 209, 220), or alternatively a name in the IPsec passage of *H.235* merely corresponding to a "call signalling channel," (*id.* at 221), Requester now turns to a third feature in an attempt to show a "secure name" that "indicates security": the *H.235* security token passage. (*Id.* at 227.) But as discussed above with respect to claim 2, the access token and security token features are entirely distinct, and the IPsec passage discloses no use of either access tokens or security tokens. Thus, even if one were to incorrectly assume that *H.235* could be incorporated by reference to show a "secure name" that "indicates security," Requester has improperly mixed and matched various distinct components of various different references in attempting to meet the claim language. *Net MoneyIn, Inc.*, 545 F.3d at 1369 (for anticipation, a reference must disclose "all of the limitations arranged or combined in the same way as recited in the claim").

Furthermore, Requester bases its "secure name" arguments regarding the *H.323* access token section and the *H.235* IPsec passages on extraneous features that merely shield names from other entities. Thus, the combined *H.323* references do not disclose that the names themselves indicate any security. (Keromytis Decl. ¶ 114.) Accordingly, the rejection should therefore be withdrawn.

g. Dependent Claim 5

As discussed above, the combined *H.323* references fail to disclose "receiving a message containing the network address *associated with the secure name of the second device*," as recited in claim 2. For the additional claim 5 feature of "receiving the message in encrypted form," Requester relies exclusively on the IPsec passage of *H.235*. But because the address returned in the IPsec passage corresponds to a "call signalling channel," rather than the endpoint earlier identified as the "second device," this passage fails to support the rejection, and the patentability of claim 5 should be confirmed. (*Id.* at ¶ 115.)

h. Dependent Claim 9

Without providing any shred of support, Requester makes the conclusory assertion that any alleged communication link would be initiated automatically. Mere attorney argument fails to support the § 102(b) rejection, as anticipation requires that "each and every element as set forth in the claim [be] found, either expressly or inherently described, in a single prior art reference." *Verdegaal* 814 F.2d at 631. The rejection should be withdrawn.

i. Dependent Claims 10 and 11

The Office asserts that the tunneling features of claims 10 and 11 are disclosed by the "Encapsulation" passage of *H.323*. (OA at 11-12, quoting *H.323* 59.) But this passage does not disclose *receiving any message containing a network address* "through tunneling," as recited in claim 10, or "in the form of at least one tunneled packet," as recited in claim 11. (Keromytis Decl. ¶ 116.) This is unsurprising, because the tunneling discussed on page 59 involves H.245 channels and messages, while the gatekeeper (alleged to correspond to the "secure name service") communicates with endpoints through H.225 signalling. (*H.323* 27.) The Office and Requester do not identify any additional passage disclosing these combined features, as the *H.235* IPsec passage cited in the Request only discloses an address corresponding to a "call signalling channel"—not an endpoint (*i.e.*, alleged "second device")—as discussed above. (*See* OA at 11-12; Req. at 231.) Thus, the rejections should be withdrawn.

j. Dependent Claim 13

Requester's argument is belied by the very passage it cites. *H.323* explains that its layering feature should employ a separate channel and a separate session, unlike the additional feature of claim 13, which recites that one "secure communication link includes multiple sessions." (*H.323* at 91; Keromytis Decl. ¶ 117.) Moreover, as discussed above with respect to claims 1 and 2, the combined *H.323* references do not disclose any "secure communication link," as recited in claim 13. The rejection should be withdrawn.

k. Dependent Claim 21

The combined *H.323* references have not been shown to disclose "providing an unsecured name associated with the device," as recited in dependent claim 21, for at least similar reasons as discussed above with respect to independent claim 1. Accordingly, the § 102 rejection of dependent claim 21 should be withdrawn.

l. Independent Claim 24 and Dependent Claim 25

Like claim 1, independent claim 24 recites multiple iterations of "secure name," as well as "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device." Accordingly, these features are not disclosed in the combined *H.323* references for similar reasons discussed above regarding claim 1. And similar to the "secure communication link" of claims 1 and 2, independent claim 24 recites "sending a message securely." Accordingly, this feature is not disclosed in the combined *H.323* references for similar reasons discussed above regarding claims 1 and 2. Thus, the rejection of claim 24 should be withdrawn, as well as the rejection of claim 25, which depends from claim 24 and includes all of its features.

m. Independent Claim 26 and Dependent Claim 27

Similar to claim 1, independent claim 26 recites multiple iterations of "secure name" and "unsecured name," as well as "receiving at the unique network address associated with the secure name of the first device a message from a second device requesting the desire to securely communicate with the first device." Accordingly, these features are not disclosed in the combined *H.323* references for similar reasons discussed above regarding claim 1. And similar to the "secure communication link" of claims 1 and 2, independent claim 26 recites "sending a message securely." Accordingly, this feature is not disclosed in the combined *H.323* references for similar reasons discussed above regarding claims 1 and 2.

Requester additionally fails to identify any "unique network address," as recited in claim 26, that corresponds to an alleged secure name (*i.e.*, an access-token-protected alias address). Instead, Requester generically quotes registration features from the combined *H.323* references without addressing how or whether these passages disclose the claimed feature of "a unique network address." (Req. at 248-53.)

Thus, the rejection of claim 26 should be withdrawn, as well as the rejection of claim 27, which depends from claim 26 and includes all of its features.

n. Independent Claim 28

Like claim 1, independent claim 28 recites multiple iterations of "secure name." This feature is not disclosed for similar reasons as discussed above regarding claim 1. And like claim 2, claim 28 recites "sending a message … requesting a network address associated with a secure name of a device" and "receiving a message containing the network address associated with the secure name." These features are not disclosed in the combined *H.323* references for similar reasons as discussed above regarding claim 2. And like claims 1 and 2, claim 28 further recites "sending a message to the network address associated with the secure name of the device using a secure communication link."

This feature is not disclosed in the combined *H.323* references for similar reasons discussed above regarding claims 1 and 2.

o. Independent Claim 29

Like claim 1, independent claim 29 recites multiple iterations of "secure name." This feature is not disclosed for similar reasons as discussed above regarding claim 1. Claim 29 also recites "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." Accordingly, it is not disclosed in the combined *H.323* references for similar reasons discussed above regarding claim 1. And similar to the "secure communication link" of claims 1 and 2, independent claims 29 recites "sending a message securely." Accordingly, this feature is not disclosed in the combined *H.323* references for similar reasons discussed above regarding claims 1 and 2.

In view of the above, the § 102(b) rejections of claims 1-29 based on the combined *H.323* references should be withdrawn.

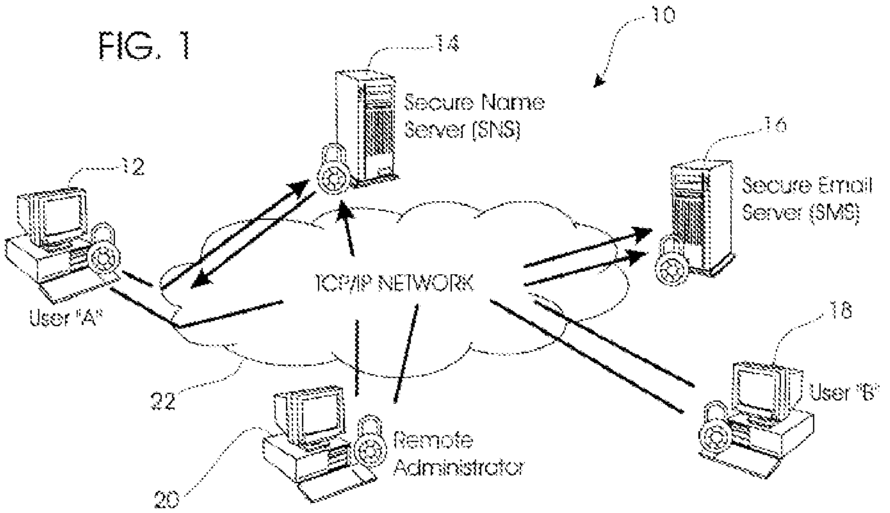
L. The Rejection of Claims 1-29 Under 35 U.S.C. § 103 Based on *Johnson* in view of *RFC 2131*, *RFC 1034*, and *RFC 2401* Should Be Withdrawn (Issue 13)

The Office Action rejects claims 1-16 and 18-29 under 35 U.S.C. § 103 based on *Johnson* in view of *RFC 2131*, *RFC 1034*, and *RFC 2401*. (OA at 12.) For the reasons discussed below, this rejection should be withdrawn and the claims should be confirmed.

1. Overview of *Johnson*

Johnson generally relates to "a secure electronic mail communication system . . . for use in communicating over networks where secure information exchange is required." (*Johnson* 1:20-23.) With reference to Fig. 1, reproduced below, *Johnson* discloses that the secure mail server 16 obtains a dynamic address from the connecting network 22 and notifies the secure name server 14 of the obtained dynamic address. (*Johnson* 6:25-34.)

FIG. 1



When a first user 12 desires to send an email to a second user 18, the first user 12 uses his "logon protocol combination to access the secure name server 14 over the connecting network 22" (*Johnson* 7:13-14), which in one embodiment may include selecting a "fixed address/name" of the secure name server 14. (*Johnson* 11:23-24.) The first user 12 "obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14" (*Johnson* 7:15-17); in one embodiment the "secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message." (*Johnson* 8:4-6.) The first user 12 then uses "his ID/password combination and the dynamic address to log onto the secure electronic mail server 16." (*Johnson* 7:20-22.) "[T]he first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16." (*Johnson* 7:23-27.) A second user may subsequently use his "logon protocol to obtain the dynamic address of the electronic mail server 16 from the secure name server 14 and then access the secure electronic mail server 16 with his ID/Password combination." (*Johnson* 7:31-35.) Thus, "the first user 12 and the second user 18 never communicate directly." (*Johnson* 7:54-55.)

2. Overview of RFC 2131, RFC 1034, and RFC 2401

RFC 2131 generally relates to a Dynamic Host Configuration Protocol (DHCP) that "provides a framework for passing configuration information to hosts on a TCPIP network." (*RFC 2131* at 1.) *RFC 1034* generally relates to "an introduction to the Domain Name System (DNS)." (*RFC 1034* at 1.) *RFC 2401* generally relates to a Security Architecture for the Internet Protocol that "addresses security only at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms." (*RFC 2401* at 3.)

3. Independent Claim 1

a. The References Do Not Disclose or Suggest "A First Device Associated with a Secure Name and an Unsecured name"

Claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." *Johnson* does not disclose these features for several reasons.

First, *Johnson* does not disclose any "secure names." As explained above regarding *Provino*, (*see supra* Section III.I.2, "secure names" are those names used to communicate securely that are resolved by a secure name service (*i.e.*, a service that both resolves a name into a network address and further supports establishing a secure communication link). The secure name server 14 in *Johnson*, on the other hand, is a conventional name server of the type distinguished in the '181 patent specification and does not qualify as a "secure name service" that can resolve "secure names." (Keromytis Decl. ¶ 121.) Instead, when provided with the name of secure mail server 16, the secure name server 14 merely returns the dynamic address of the secure mail server 16. (*Id.*) *Johnson* does not disclose that secure name server 14 provides any further support for establishing a secure communication link. (*Id.*) Accordingly, its operation is conventional, it is not a "secure name service" in the context of the '181 patent, and the names disclosed in *Johnson* are not "secure names." (*Id.*)

Second, the Office and Requester allege that the secure mail server 16 of *Johnson* corresponds to the claimed "first device," and that a name allegedly registered "by the secure mail server with the secure name server is a 'secure name' . . . because it requires, for example, authorization to access and is protected through encryption." (Req. at 272.) Without addressing whether a "secure name" requires "authorization to access and is protected through encryption," if that is the standard the Office is applying, *Johnson* does not meet it, because *Johnson* does not teach or suggest that the name of secure mail server 16 is protected through authorization and encryption. (Keromytis Decl. ¶ 122.) Instead, the user accessing the secure name server 14 must presumably already know the name of the secure mail server 16 before the alleged authorization and encryption ever happens, because if the user did not already know the name, it would not know how to request any information regarding the secure mail server 16 from secure name server 14. (*Id.*) There is no disclosure in *Johnson* regarding how the user initially learns this name, whether authorization is required before obtaining the name, or whether encryption is used in providing the name. (*Id.*) Accordingly, Requester and the Office have not demonstrated that *Johnson* discloses or suggests a "secure name" even under their own interpretation of that term.

Third, the Office and Requester incorrectly allege that the claimed "unsecured name" is disclosed by a domain name of the secure name server 14 that is allegedly registered with a DHCP server (as allegedly taught by *RFC 2131*) or in a public DNS system (as allegedly taught by *RFC 1034*). (Req. at 273-74.) This argument misses the mark for at least two reasons. One is that Requester never argues that secure name server 14 is the claimed "first device associated with a secure name and an unsecured name." Instead, Requester alleges that secure mail server 16 is the claimed "first device." Thus, it is irrelevant whether secure name server 14 has an unsecured name, as it has no bearing on the claims. The second reason is that both allegations (regarding registration of secure name server 14 with a DHCP server or in the public DNS system) appear to rely on the premise that the secure name server 14 must have a registered domain name, which the Office and Requester allege is "necessary to the invention of Johnson" for *Johnson* to be used in "communications over the Internet." (Req. at 274.) This premise is incorrect because a registered domain name is not a prerequisite for communications over the Internet. (Keromytis Decl. ¶ 124.) In fact, communications over the Internet existed well before the creation of *RFC 1034* that is asserted by the Office and Requester as disclosing domain name registration. (*Id.*)

Finally, the Office and Requester allege that "the secure mail server has a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an 'unsecured name'." (Req. at 274.) Requester cites no support for this statement (*see id.*), and the statement is incorrect because the secure mail server 16 is only disclosed to have its name registered in secure name server 14. (Keromytis Decl. ¶ 125.) Accordingly, the Office and Requester have not shown that secure mail server 16 has an "unsecured name," as claimed.

The Office and Requester do not allege that *RFC 2401* cures any of these deficiencies of *Johnson*, *RFC 2131*, and *RFC 1034*. (*See* Req. at 270-75.) Thus, the claimed feature of "a first device associated with a secure name and an unsecured name" is not rendered obvious by *Johnson*, *RFC 2131*, *RFC 1034*, or *RFC 2401*, alone or in combination.

b. The References Do Not Disclose or Suggest "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire[] to Securely Communicate with the First Device"

Claim 1 further recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." Since *Johnson* and the other cited references do not disclose or suggest a "secure name" for the reasons discussed above, the references do not render obvious this claimed feature.

The references are also lacking regarding the "message from a second device of the desire[] to securely communicate with the first device." The Office and Requester contend that the claimed "message" is *Johnson's* email message from first user 12 to second user 18. (Req. at 275; *see Johnson* 7:10-11.) This communication is provided by the first user 12 to second user 18's mailbox on secure mail server 16. (*Johnson* 7:20-27.) Since the content of the message is destined for second user 18, *Johnson* does not disclose that it contains any information intended for use by secure mail server 16 (*i.e.*, the alleged "first device"), let alone any indication of a desire to securely communicate with the secure mail server 16. The Office and Requester do not allege that the other cited references cure this deficiency of *Johnson*. (*See* Req. at 274-75.) Thus, the Office and Requester have not demonstrated obvious in view of the cited references.

c. The References Do Not Disclose or Suggest "Sending a Message over a Secure Communication Link from the First Device to the Second Device"

Claim 1 further recites "sending a message over a secure communication link from the first device to the second device." The Office and Requester allege that the email message of the first user 12 (alleged "second device") that is transmitted to the secure mail server 16 (alleged "first device") discloses or suggests this feature. (Req. at 274-275.) The Office and Requester have things reversed. (Keromytis Decl. ¶ 127.) The email message of the first user 12 (alleged "second device") is sent to a mailbox on the secure mail server 16 (alleged "first device"); it is not sent from the alleged "first device" to the alleged "second device" as required by the claim. (*Id.*)

Furthermore, the Office and Requester allege that the email of the first user 12 is both "a message from a second device of the desire[] to securely communicate," and "a message . . . from the first device to the second device." (Req. at 275.) However, one of ordinary skill in the art would recognize that the email from the first user 12 cannot be both "a message from a second device" and "a message . . . to the second device." (Keromytis Decl. ¶ 127.) Thus, the Office and Requester have not shown that *Johnson* discloses or suggests "sending a message . . . from the first device to the second device," as recited in claim 1. The Office and Requester do not allege that the other cited references cure these deficiencies of *Johnson*. (*See* Req. at 275-76.)

For the many reasons identified above, the Office and Requester have not demonstrated obviousness in view of *Johnson*, *RFC 2131*, *RFC 1034*, or *RFC 2401*, either alone or in combination. Accordingly, the rejection of claim 1 under § 103 should be withdrawn.

4. Independent Claim 2

Claim 2 recites, among other things, "a second device having a secure name" and "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." The Office and Requester allege that the claimed "second device" is *Johnson's* secure mail server 16 and the claimed "first device" is *Johnson's* first user 12. (Req. at 281.) These allegations are otherwise substantially the same as the allegations above regarding similar features of independent claim 1. (*See* Req. at 278 and 282.) Thus, at least for reasons similar to those discussed above with regard to independent claim 1 (for example, that *Johnson* does not disclose any "secure names"), these claimed features are not rendered obvious by *Johnson*, *RFC 2131*, *RFC 1034*, or *RFC 2401*, alone or in combination. Accordingly, the rejection of claim 2 under § 103 should be withdrawn.

5. Dependent Claims 3-16 and 18-23

Claims 3-16 and 18-23 directly or indirectly depend from claim 2, and therefore include all of the features of claim 2. Thus, for at least the reasons discussed above with regard to claim 2, *Johnson*, *RFC 2131*, *RFC 1034*, and *RFC 2401*, alone or in combination, do not render obvious claims 3-16 and 18-23. The patentability of claims 3, 7, 9-11, 13-16, 21, and 22 is further supported by the additional reasons provided below.

6. Dependent Claim 3

Claim 3 recites, among other things, "the secure name of the second device is a secure domain name." As previously discussed, the Office and Requester have not established that the secure mail server 16 (alleged "second device") has a "secure name." Nonetheless, the Office and Requester allege that the Domain Name System ("DNS") teachings of *RFC 1034*, combined with *Johnson*, disclose or suggest that the name of the secure mail server 16 can be a secure domain name. (Req. at 283-284.) In support of this allegation, the Office and Requester combine *RFC 1034*'s teaching of an authoritative name server with the secure name server 14 of *Johnson* to conclude that the secure name server 14 is "the authoritative name server for the protected network." (Req. at 283-284.) The Office and Requester, however, provide no reasoning supporting this conclusory allegation. (*See id.*) There is no indication of how *Johnson* would determine which of its multiple name servers, if any, would function as the authoritative name server. (*See id.* at 282-84; *see also* Keromytis Decl. ¶ 130.)

The Office and Requester do not allege that the other cited references cure these deficiencies of *Johnson* and *RFC 1034*. (*See* Req. at 282-84.) Thus, claim 3 is not obvious.

7. Dependent Claim 7

Claim 7 recites, among other things, "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." The Office and Requester allege that a secure communication link would not be utilized during registration of a secure mail server 16 in *Johnson's* embodiment where the secure name server 14 and the secure mail server 16 reside on the same computer system, but that a secure communication link is allegedly utilized during the registration of the secure mail server 16 in *Johnson's* other embodiments. (Req. at 287.) However, there is no disclosure or suggestion in *Johnson* that the registration process changes if the secure name server 14 and the secure mail server 16 reside on the same computer system. (Keromytis Decl. ¶ 131.) Instead, *Johnson* discloses that in this embodiment, "two separate communication lines would be necessary to allow for the fixed address of the secure name server while providing for a dynamic address of the secure mail server." (*Johnson* 12:20-25.) Accordingly, one of ordinary skill in the art would recognize that the servers 14 and 16 still communicate over the network via the two separate communication lines, thus warranting no change in their operation and certainly no change that would result in communications having weakened or no security. (Keromytis Decl. ¶ 132.) Consequently, the Office and Requester have not shown that the registration process in any of the embodiments of *Johnson* utilizes a non-secure communication link. The Office and Requester do not allege that the other cited references cure these deficiencies of *Johnson* (*see* Req. at 286-87), so claim 7 is not obvious.

8. Dependent Claims 9-11 and 13-16

The Requester's proposed rejections for claims 9-11 and 13-16, which the Office adopted (OA at 12), are deficient in many ways. For example, the Office and Requester allege that one of ordinary skill in the art would be motivated to combine *Johnson* with *RFC 2401* to, for example, "facilitate secure communications between devices." (*See, e.g.*, Req. at 293.) However, combining *RFC 2401* with *Johnson* would change the principle of operation of *Johnson's* system, and therefore there is no motivation to combine *Johnson* with *RFC 2401*. In particular, *Johnson* discloses a system that is allegedly used in "network communications where security is required," (*Johnson* 1:26.), while *RFC 2401* discloses a "[s]ecurity Architecture for the Internet Protocol." (*RFC 2401* at 2.) Accordingly, replacing *Johnson's* system (that is allegedly used in network communications where security is required) with *RFC 2401's* security architecture would change the principle of operation of *Johnson's* system, (*i.e.*, the proposed combination would change the manner in which *Johnson's* system is used in "network communications where security is required"). Furthermore, the security architecture of *RFC 2401*, may be redundant to, and may not be interoperable with, the system of *Johnson*. One of ordinary skill in the art would recognize the folly in this combination and would not have been motivated to make the combination. *See In re Ratti,* 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

9. Dependent Claim 21

Claim 21 recites, among other things, "providing an unsecured name associated with the device." The Office and Requester allege that *Johnson* combined with *RFC 2131* and *RFC 1034* discloses or suggests this feature, based on the premise that the secure name server 14 of *Johnson* has a DNS name registered with a public DNS system, as allegedly taught by *RFC 1034*. (Req. at 298-299.) This argument is incorrect for the reasons discussed above regarding claim 1, including that the Office and Requester have not identified any device having both secure and unsecured names, and because there is no suggestion or motivation to combine the DNS teachings of *RFC 1034* with the secure name server 14 of *Johnson* since the proposed combination would render *Johnson* unsatisfactory for its intended purpose. (*See supra* Section III.L.3.) Accordingly, the rejection of claim 21 should be withdrawn.

10. Dependent Claim 22

Claim 22 recites, among other things, "wherein the secure name is registered prior to the step of sending a message to a secure name service." The Office and Requester completely fail to address the claimed feature of the secure name being registered "prior to the step of sending a message to a secure name service," as recited in dependent claim 22. (*See* Req. at 299-300.) Accordingly, the rejection is deficient and should be withdrawn. *See Ex Parte Karl Burgess*, Appeal 2008-2820, 2009 WL 291172, at *3 (to support an obviousness rejection, "all of the claim limitations must be taught or suggested by the prior art applied and that all words in a claim must be considered . . . .").

11. Independent Claim 24

Requester's proposed rejection for claim 24, which the Office adopted (OA at 12), is deficient in several ways. For example, as explained regarding claim 1, the cited references do not disclose any "secure names" because there is no secure name service to resolve secure names. (*See supra* Section III.L.3.) Thus, the proposed combination does not teach the claimed "secure name" recited in several places in claim 24. Claim 24 also recites "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." It is not disclosed in the cited references for the same reasons discussed above regarding the similar feature of claim 1. (*See supra* Section III.L.3.)

Claim 24 further recites "sending a message securely from the first device to the second device." The Office and Requester allege that the transmission of the email message of the first user 12 (alleged "second device") to the designated recipient's box on the secure mail server 16 (alleged "first device") discloses or suggests this feature of claim 24. (Req. at 303-304.) Once again Requester has things reversed, as the claim recites "sending a message securely from the first device to the second device," not sending a message from the second device to the first device. Accordingly, the Office and Requester have not shown that *Johnson* discloses or suggests this feature, and they have not alleged that the other cited references cure this deficiency of *Johnson*. (*See* Req. at 301-04.)

For at least these reasons, claim 24 is not obvious in view of *Johnson*, *RFC 2131*, *RFC 1034*, or *RFC 2401*, alone or in combination.

12. Dependent Claim 25

Claim 25 depends from claim 24 and is patentable for at least the reasons discussed above regarding claim 24. Claim 25 also recites, among other things, "sending a message securely comprises sending the message from the first device to the second device using a secure communication link." The Office and Requester completely fail to address this aspect of claim 25. (*See* Req. at 304-05.) Thus, the rejection is deficient and should be withdrawn. *See Ex Parte Karl Burgess*, Appeal 2008-2820, 2009 WL 291172, at *3 (to support an obviousness rejection, "all of the claim limitations must be taught or suggested by the prior art applied and that all words in a claim must be considered . . . .").

13. Independent Claim 26

Claim 26 recites, among other things, "a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device"; "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device"; and "from the first device sending a message securely from the first device to the second device." The Office's and Requester's allegations that these features are disclosed by the cited references are substantially the same as those provided in support of the rejections of one or more previously discussed independent claims (*e.g.*, independent claim 1). (*See* Req. at 305-310.) For at least reasons similar to those discussed above regarding one or more previously discussed independent claims, the Office and Requester have not shown that the cited references, alone or in combination, disclose or suggest these features of claim 26.

14. Dependent Claim 27

Claim 27 depends from claim 26, and therefore includes all of the features of claim 26. Thus, for at least the reasons discussed above regarding claim 26, *Johnson*, *RFC 2131*, *RFC 1034*, or *RFC 2401*, alone or in combination, do not render obvious the features of claim 27.

15. Independent Claim 28

Like claim 1, independent claim 28 recites multiple instances of "secure name." This feature is not disclosed in the cited references for at least the same reasons discussed above regarding claim 1. And like claim 2, claim 28 further recites a "secure name service." This feature is not disclosed in the cited references for the same reasons discussed above regarding claim 2. Accordingly, the rejection of claim 28 under § 103 should be withdrawn.

16. Independent Claim 29

Independent claim 29 recites multiple instances of "secure name." This feature is not disclosed in the cited references for at least the same reasons discussed above regarding claim 1. Claim 29 also recites "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." Accordingly, it is not disclosed in the cited references for the same reasons discussed above regarding the similar feature of claim 1. The rejection of claim 29 under § 103 should be withdrawn.

M. Secondary Considerations of Nonobviousness

"Objective evidence relevant to the issue of obviousness <u>must</u> be evaluated by Office personnel." M.P.E.P. 2141(II) (emphasis added). The Federal Circuit "has repeatedly emphasized that the objective indicia [of nonobviousness] constitute 'independent evidence of nonobviousness.'" *Mintz v. Dietz & Watson*, 679 F.3d 1372, 1378 (Fed. Cir. 2012) (citations omitted). "Indeed, objective indicia 'may often be the most probative and cogent evidence of nonobviousness in the record,' and "'may often establish that an invention appearing to have been obvious in light of the prior art was <u>not</u>.'" *Id.* (emphasis added). Objective indicia includes expert skepticism, commercial success, acceptance by others in the field, praise by others, failure of others, and long-felt need. *Id.* at 1379; M.P.E.P. 2145. Here, even if the Office had established a *prima facie* case of obviousness regarding any of claims 1-29 (which it has not), there is substantial evidence to rebut any finding of obviousness.

Prior to the effective filing date of the '181 patent, there was a significant concern for security in computer network communications. (Short Decl. ¶ 3.) The widespread connectivity between computers led to many security breaches, as well as growing concerns regarding the safety of confidential information sent over computer networks. (*Id.*) For example, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. (*Id.* at ¶¶ 8, 11.) Specifically, remote access was "a nightmare" for support desks, and adding the commercially available VPN software was even more difficult. (*Id.* at ¶ 11.) The computer and internet security industries were forced to choose between an easy-to-use system and a system with the security of a VPN, but they could not have both. (*Id.* at ¶ 9.)

Many organizations tried and failed to provide a solution that allowed a user to easily and conveniently enable secure communications. (*Id.* at ¶ 5.) For example, the Defense Advanced Research Projects Agency ("DARPA") funded various research programs that were focused on the need to provide easy-to-enable secure communications. (*Id.* at ¶ 4.) One such program received funding of over $128 million between 1998 and 2000. (*Id.*) DARPA contracted with some of the most skilled organizations in the area of secured communications in an effort to meet its security needs, however, none of these organizations was able to produce a solution during the relevant time frame that was close to what is disclosed and claimed in the '181 patent and its patent family. (*Id.* at ¶ 5.) That is, even with over $128 million invested, none of these organizations developed a solution that allowed a user to easily and conveniently enable secure communications. (*Id.*)

Despite the failure of others, Science Applications International Corporation ("SAIC") (the original assignee of the application that led to the '181 patent) recognized a long-felt need for easily enabled secure communications, and invested approximately $2 million for research and development of technology that led to the inventions disclosed and claimed in the '181 patent. (*Id.* at ¶ 7.) The year the inventions claimed in the '181 patent were developed, SAIC spent approximately 85% of its entire research and development budget for that year on developing these and other similar inventions. (*Id.*) Understandably, the technology developed by SAIC engineers was met with skepticism by those skilled in the art. (*Id.* at ¶ 14.) For example, a program manager for DARPA informed Edmund Munger, a co-inventor of the '181 patent, that the technology would never be adopted. (*Id.* at ¶ 15.) Additionally, the IT offices of many large companies and institutions expressed skepticism that secure connections could ever be enabled easily by regular computer users. (*Id.*)

Ultimately, the technology of the '181 patent was adopted, and even received praise by those in the field. (*Id.* at ¶ 16.) For example, the CEO of Network Solutions during the relevant time praised and expressed significant interest in the technology, and would have invested but for a change in circumstances at his company (*i.e.*, acquisition by VeriSign). (*Id.*) Cambridge Strategic Management Group ("CSMG") also substantiated the value of the technology. (*Id.* at ¶ 7.)

The claimed inventions have also experienced significant commercial success. In particular, SafeNet, a leading provider of Internet security technology that is the de facto standard in the VPN industry, entered into a portfolio license with the original owner of the '181 patent on July 2002. (*Id.* at ¶ 12.) Microsoft, Aastra, Mitel, and NEC have all since entered into patent licensing agreements with VirnetX that include the '181 patent. (*Id.* at ¶ 16.) Indeed, Microsoft was found to willfully infringe two of the patents in the Munger patent family, leading to a damages award of over $100 million dollars. (*Id.* at ¶ 12.)

By providing systems and methods for easily enabling secure communications, the inventions of the '181 patent have satisfied a long-felt need and succeeded where others failed. (*Id.* at ¶ 11.) Moreover, the commercial success and praise of the technology despite a disproportionate investment in that technology and skepticism by those skilled in the art, rebuts any finding that the claimed inventions would have been obvious. *See Mintz v. Dietz & Watson*, 679 F.3d at 1379-80.

IV. Conclusion

For at least these reasons, VirnetX requests reconsideration and withdrawal of the rejections in the Office Action and confirmation of the patentability of all of the claims of the '181 patent.

VirnetX notes that the Request, Order, and Office Action contain a number of assertions and allegations concerning the '181 patent disclosure, '181 patent claims, and the cited references. VirnetX does not subscribe to any assertion or allegation in the Request, Order, or Office Action regardless of whether it is addressed specifically herein.

Please grant any extension of time necessary, and charge our Deposit Account No. 502624 any fees or credit any overcharges relating to this Response.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/John A. Hankins/
John A. Hankins, Reg. No. 32,029
Toby H. Kusmer, P.C., Reg. No. 26,418
Kenneth C. Cheney, Reg. No. 61,841
Ricky K. Chun, Reg. No. 63,371
Michael G. Dreznes, Reg. No. 59,965
McDermott Will & Emery LLP
Attorneys for Patent Owner

4 Park Plaza, Suite 1700
Irvine, California 92614-2559
Telephone: (949) 851-0633
Facsimile: (949) 851-9348
Date: September 4, 2012

Please recognize our Customer No. 23630 as our correspondence address.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U. S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF DR. ROBERT DUNHAM SHORT III

I, Robert Dunham Short III, declare as follows:

1. I have been the Chief Technology Officer of VirnetX Inc. ("VirnetX") since June 2010 and the Chief Scientist for VirnetX since May 2007. Prior to joining VirnetX, from 1994 to April 2007, I held various positions including Assistant Vice President and Division Manager at Science Applications International Corporation ("SAIC"). Prior to SAIC, I worked at ARCO Power Technologies Inc., Sperry Corporate Technology Center, and Sperry Research Center. I have a Ph.D. in Electrical Engineering from Purdue University as well as a M.S. in Mathematics and a B.S. in Electrical Engineering from Virginia Tech.

2. I am one of the named inventors of U.S. Patent No. 8,051,181 ("the '181 patent"), which I understand is the subject of the above-identified reexamination proceedings. I am familiar with the '181 patent, including its claims.

3. Prior to and at the time of the inventions claimed in the '181 patent, there was a significant and increasing concern with the security of computer network communication. The widespread connectivity between computers that was enabled by the swift increase in network access in homes and businesses also led to many security breaches as well as concerns regarding the safety of confidential information sent over computer networks. This problem received significant attention from the research and development community. Practical experience showed that there was a need for a system that could be easily and correctly used to enable secure communications, because a

system that made it difficult for an end-user to enable secure communications would likely lead to a lack of use or incorrect use. The inventions disclosed and claimed in the '181 patent and other patents in this family met this need. For instance, the inventions disclosed and claimed in the '181 patent include systems and methods of securely communicating with a device having a secure name. As an example, independent claim 1 recites "receiving, at a network address corresponding to [a] secure name associated with [a] first device, a message from a second device of the desired to securely communicate with the first device; and sending a message over a secure communication link from the first device to the second device." ('181 patent 55:36-41.) Likewise, independent claim 2 recites "sending a message to a secure name service, the message requesting a network address associated with [a] secure name of [a] second device" and "sending a message to the network address associated with the secure name of the second device using a secure communication link." (*Id.* at 55:44-52.) Independent claim 28 recites similar features. (*Id.* at 58: 7-14.) And, independent claim 24 recites "receiving at [a] network address associated with [a] secure name of [a] first device a message from a second device of the desire to securely communicate with the first device; and sending a message securely from the first device to the second device." (*Id.* at 56:62-67.) Independent claims 26 and 29 recite similar features. (*Id.* at 57:17-22, 58:15-24.)

4. As one example of the manifestation of the long-felt need, the Defense Advanced Research Projects Agency ("DARPA") funded various research programs to further the science and technology of information assurance and survivability. DARPA programs, such as the "Information Assurance" and "Dynamic Coalitions" programs, were focused on the need to provide easy-to-enable secure communications. These projects received significant funding to be spent developing technologies that could solve this need. For example, one such project entitled "Next Generation Internet" received funding in fiscal year 1998 of approximately $39.3 million, in fiscal year 1999 of approximately $49.5 million, and in fiscal year 2000 of approximately $40 million. (Ex. B-1 at VNET00219302, 319-321.) Another program funded by DARPA, "Dynamic Coalitions," was created to address the ability of the Department of Defense to quickly and easily enable secure communications over the Internet. (*See, e.g.*, Ex. B-2 at VNET00219244, 284, 298-299, 593, 625.)

5. According to DARPA officials at the time, "existing group membership protocols d[id] not support the security needs of multidimensional organizations. The overarching challenge [wa]s creating secure groups rapidly. This [wa]s a significant issue when countries [we]re faced with an operation that require[d] immediate multinational attention." (Ex. B-3 at 1.) DARPA contracted with some of the most skilled organizations in the area of secured communications in an effort to meet its security needs (e.g., NAI Labs, a division of PGP Security, Network Associates Incorporated, Los

Angeles, and the Microelectronics Center of North Carolina, Research Triangle Park, North Carolina, as well as Johns Hopkins University, Baltimore; Northeastern University, Boston; and Veridian-PSR, Arlington, Virginia). (*Id.* at 1.) In all, more than 15 organizations were researching the various components that made up the programs initiated by the Department of Defense. (*Id.*) However, none of these prestigious institutions came up with a solution, during the relevant time frame, close to what is disclosed and claimed in the '181 patent. (*Id.* at 1-4.) That is, they did not develop a solution that enabled secure communication with a device having a secure name.

6. As a second example of the long-felt need for the inventions of the '181 patent, In-Q-Tel, which is a venture capital firm that invests in companies developing cutting edge technology aimed at supporting the United States intelligence community, including the Central Intelligence Agency (CIA), funded the original development of the technology with approximately $3.4 million. In-Q-Tel's willingness to enter into a relationship with SAIC (the original assignee of the application that led to the '181 patent) for the development of this technology further evidences a long-felt need for technology that made it easy and convenient to enable secure communications.

7. A third example was the extent to which SAIC internally funded the research and development of the technology. When I was employed at SAIC, its business model was to sell hours to the federal government. SAIC was not structured to bring products to the market, which typically requires significant internal investments in research and development. In an average year during the development of the technology that led to the '181 patent, SAIC would spend approximately $2 million on internal research and development efforts. In the case of the technology claimed in the '181 patent, SAIC invested $1.7 million, which represents almost the entirety of SAIC's internal research and development budget for one whole year. A technology review committee also approved our team's patent development efforts and costs on an ongoing basis. A third party (Cambridge Strategic Management Group or CSMG) also substantiated the value of the technology. Moreover, a significant percentage of all of SAIC's patent development efforts have focused on this technology. I understand that SAIC spent one-third of its total patent portfolio efforts on our patent portfolio at that time.

8. In fact, as demonstrated in an article written before the claimed inventions of the '181 patent, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. (Ex. B-4 at 1.) In that time period, remote access was "a nightmare for support desks. Staffers never kn[e]w what combination of CPU, modem, operating system and software configuration they [were] going to have to support," and adding the commercially-available VPN software only made matters worse. (*Id.*)

9. This article precisely captured the computer and Internet security industry's attitude toward the tradeoff between the ease of use of a secure system, such as a VPN system, for the average computer user and the security that the VPN system provided. The article recognized that the "ease of installation isn't always a good thing: In many cases, the easier the client is to install, the less secure it is." (*Id.* at 2.) The claimed inventions of the '181 patent, which provide systems and methods of securely communicating with a device having a secure name, combine both ease of use and security aspects without sacrificing one or the other.

10. Moreover, many others before and around the time of the inventions claimed in the '181 patent have attempted to solve the need of easy-to-use methods of enabling secure communications over the Internet. But, as discussed above, many of these attempts have failed. For example, despite investing enormous amounts of money and enlisting the resources of numerous prestigious institutions and their talented employees, DARPA's projects still fell far short of the claimed inventions of the '181 patent. (*See* ¶¶ 4-5, *supra*.)

11. Additionally, as discussed above, no one had yet achieved the results of the claimed inventions of the '181 patent in that time period, because remote access was "a nightmare" for support desks to handle, and adding the commercially-available VPN software was even more difficult. In fact, at this time, the security industry generally viewed ease of use and VPN security as mutually exclusive. (*See* ¶¶ 8-9, *supra*.) By providing systems and methods of securely communicating with a device having a secure name, the inventions of the '181 patent provided a solution for easily establishing secure communication links without sacrificing security, thereby succeeding where others failed.

12. The claimed inventions of the '181 patent have been commercially successful, for example, through the licensing revenues they have generated for VirnetX. In July 2002, SafeNet, a leading provider of Internet security technology that is the de facto standard in the VPN industry, entered into a portfolio license with SAIC to incorporate features into SafeNet's underlying VPNs. SafeNet licensed the patents because of features disclosed and claimed in the patents, including those in the '181 patent. Microsoft has also entered into a similar license that includes the '181 patent. Microsoft entered into its license with VirnetX after it was found to have infringed two other VirnetX patents in the same family, resulting in a damages award of over one hundred million dollars, leading ultimately to a license agreement of two hundred million dollars. And on May 3, 2012, Aastra USA, Inc. entered into a license with VirnetX that includes the '181 patent. Likewise, on July 11, 2012, Mitel Networks Corporation entered into a license with VirnetX that also includes the '181 patent.

Then, on August 2, 2012, NEC Corporation and NEC Corporation of America entered into a license with VirnetX that also includes the '181 patent.

13. The claimed inventions of the '181 patent were also contrary to the accepted wisdom at the time of the inventions. For example, there was a general understanding that reliable security could only be achieved through difficult-to-provision VPNs and easy-to-set-up connections could not be secure. This belief was reinforced by the IT offices of many large companies and institutions, whose livelihood depended on the need for highly-trained specialists to arrange secure network connections.

14. The industry had long accepted as a fact that secure systems, such as VPN systems, would be difficult to set up, and the secure communication modes could not be easily and conveniently enabled. In a 1999 article entitled "CEOs Chew the VPN Fat" that predicted what the future held for the start-up companies that developed VPNs, the wish list did not even address the type of solutions provided by the '181 patent, such as systems and methods of securely communicating with a device having a secure name. (Ex. B-5 at 1-2.)

15. The technology of the '181 patent was also met with skepticism by those skilled in the art who learned of our inventions. Sami Saydjari, a program manager for DARPA, informed Edmund Munger, a co-inventor of the '181 patent, that our technology would never be adopted. Moreover, the IT offices of many large companies and institutions expressed skepticism that secure connections could ever be enabled easily by regular computer users.

16. Several events also demonstrate praise for the inventions in the '181 patent by those in the field. As discussed above, SAIC invested a disproportionately large percentage of its internal resources in the technology. SafeNet, Microsoft, Aastra, Mitel, and NEC have all licensed the technology of the '181 patent. A study done by CSMG also praised the inventions. Jim Rutt at Network Solutions, which was acquired by Verisign, praised and expressed significant interest in the technology and would have invested but for a change in circumstances at his company.

17. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the '181 patent.

Dated: August 31, 2012

By: /Robert Dunham Short III/
Robert Dunham Short III

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Declaration of Angelos D. Keromytis, Ph.D.

I declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

I, ANGELOS D. KEROMYTIS, declare as follows:

1. I have been retained by VirnetX Inc. ("VirnetX") for the above-referenced reexamination proceeding. I understand that this reexamination involves U.S. Patent No. 8,051,181 ("the '181 patent"). I further understand that the '181 patent is assigned to VirnetX and that it is part of a family of patents ("Munger patent family") that stems from U.S. provisional application nos. 60/106,261 ("the '261 application"), filed on October 30, 1998, and 60/137,704 ("the '704 application"), filed on June 7, 1999. I understand that the '181 patent is a continuation of U.S. Patent 7,188,180, which is a divisional of U.S. application no. 09/558,209 filed April 26, 2000 (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent 6,502,135, "the '135 patent"). The '135 patent is a continuation-in-part of U.S. application no. 09/429,643 (now U.S. Patent 7,010,604), which claims priority to the '261 and '704 applications.

I. RESOURCES I HAVE CONSULTED

2. I have reviewed the '181 patent, including claims 1-29. I have also reviewed a Request for *Inter Partes* Reexamination of the '181 patent filed by Apple Inc. ("Requester") with the U.S. Patent and Trademark Office ("The Office") on March 28, 2012 ("Request" or "Req.") as well as the exhibits accompanying the Request. Additionally, I have reviewed an Order Granting Request

for *Inter Partes* Reexamination of the '181 patent ("the Order") mailed on June 4, 2012 and an Office Action ("the Office Action") mailed on June 4, 2012.[1]

3. I have also studied the following documents cited in and included with the Request and/or Office Action: U.S. Patent No. 6,496,867 to Beser et al. ("*Beser*"); U.S. Patent No. 6,131,121 to Mattaway et al. ("*Mattaway*"); Lendenmann, "Understanding OSF DCE 1.1 for AIX and OS/2" ("*Lendenmann*"); U.S. Patent No. 6,557,037 to Provino ("*Provino*"); RFC 2131, "Dynamic Host Configuration Protocol ("RFC 2131"); U.S. Patent No. 6, 499, 108 to Johnson ("*Johnson*"); ITU-T H.323, "Packet-Based Multimedia Communications Systems" ("H.323"); ITU-T H.225.0, "Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems" ("H.225.0"); ITU-T H.235, "Security and Encryption for H-Series Multimedia Terminals," ("H.235"); ITU-T H.245, "Infrastructure of Audiovisual Services—Communication Procedures" ("H.323"); RFC 1034, "Domain Names—Concepts and Facilities" ("RFC 1034"); and RFC 2401, "Security Architecture for the Internet Protocol, ("RFC 2401").

4. I am familiar with the level of ordinary skill in the art with respect to the inventions of the '181 patent as of February 15, 2000, when the application for the '181 patent was filed. Specifically, based on my review of the technology, the educational level of active workers in the field, and drawing on my own experience, I believe a person of ordinary skill in art at that time would have had a master's degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security.

5. I have been asked to consider how one of ordinary skill in the art would have understood the references mentioned above. My findings are set forth below.

II. QUALIFICATIONS

6. I have a great deal of experience and familiarity with computer and network security, and have been working in this field since 1993.

7. I am currently an Associate Professor of Computer Science at Columbia University, as well as Director of the University's Network Security Laboratory. I joined Columbia in 2001 as an Assistant Professor, after receiving my M.Sc. and Ph.D. degrees in Computer Science, both from the University of Pennsylvania. My Ph.D. dissertation work was on the topic of secure access control for distributed systems and, in particular, on the management of trust in distributed computer networks.

[1] The Office Action incorporates nearly all of the Request by reference. For that reason, when I sometimes refer to "the Request" or "the Requester" I am also referring to the Office Action or the Office.

8. I received my B.Sc. in Computer Science from the University of Crete, in Greece, in 1996. During my undergraduate studies, I worked as system administrator in the Computing Center at the University of Crete. Following that, I worked as network engineer at the first commercial Internet Service Provider ("ISP") in Greece, FORTHnet SA, where I was exposed to many network security issues.

9. I have actively participated in the Internet Engineering Task Force ("IETF"), a standards-setting body for the Internet, since 1995. In the late 1990s and early 2000s, my work with the IETF was primarily within the Internet Protocol Security ("IPsec") Working Group. In addition to contributing to the specification of the IPsec standards, I wrote the first implementation of the Photuris key management protocol (now RFC 2522). I also contributed to the first open-source implementation of the IKSAMP/IKE key management protocol for the open-source BSD operating system (now RFC 2409), and developed the first such implementation for the Linux operating system. My Linux implementation, named Pluto, was adopted by the National Institute of Standards and Technology ("NIST") in 1999. In addition, my implementation of IPsec for the open-source BSD operating system is currently used by many companies and governments around the world, and serves as the basis for several commercial products that employ cryptographic communications. In 1999, I architected and implemented the first open-source framework for supporting hardware cryptographic accelerators. This framework is used in the open-source OpenBSD, NetBSD, FreeBSD, and Linux operating systems. My work in implementing firewalls and other cryptographic and network protocols has resulted in commercial systems and publications in refereed technical conferences and academic journals. I served as Working Group Secretary for the IETF IPsec Working Group (2003-2005) and as Security Area Advisor to the IETF at large (2003-2008).

10. In my current position at Columbia University, I work with a large group of graduate and postgraduate students in the area of cybersecurity. My past students now work in this field as university professors, as technical researchers for research laboratories, or as engineers for telecommunications companies. I have received federal, state, and corporate sponsorship to conduct cybersecurity research from the Department of Defense, the National Security Agency, the Defense Advanced Research Projects Agency ("DARPA"), the National Science Foundation, the Department of Homeland Security, the Air Force, the Office for Naval Research, the Army Research Office, the Department of the Interior, the National Reconnaissance Office, New York State, Google, Intel, Cisco, and others. In my ten years as a professor, I have received over 36 million dollars to support

my research in cybersecurity. I also regularly teach courses on cybersecurity, in addition to more general courses in computer science.

11. I have published over 200 technical papers in refereed journals, conferences, and workshops, all of which are directed to various areas of cybersecurity. I have also authored a book, coauthored another book, and contributed chapters for many other books that relate to cybersecurity. Between 1999 and 2010, I have drafted or codrafted eight standards documents that were published as Request for Comments ("RFCs"). Several of these RFCs are directly related to IP security. For example, RFC 6042 relates to transport layer security; RFC 5708, RFC 2792, and RFC 2704 relate to key signature and encoding for trust management; and RFC 3586 relates to IP security policy requirements. Additionally, I am a coinventor on twelve issued U.S. patents, and have several other applications pending. Most of these patents and pending applications are related to network and systems security.

12. I have chaired several international technical conferences and workshops in cybersecurity, including, for example, the International Conference on Financial Cryptography and Data Security (FC), ACM Computer and Communication Security (CCS), and the New Security Paradigms Workshop (NSPW). I have also served in over eighty technical program committees for such events. From 2004-2010, I served as Associate Editor for the premier technical journal on cybersecurity—the ACM Transactions on Information and Systems Security (TISSEC). Additionally, I have served on several advisory workshops to the United States Government on cybersecurity, including, among others, the Office of the Director of National Intelligence (ODNI)/National Security Agency (NSA) Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E) (2011), the Office of Naval Research (ONR) Workshop on Host Computer Security (2010), the Intelligence Community Technical Exchange on Moving Target (2010), Lockheed Martin Future Security Threats Workshop (2009), and the ARO/FSTC Workshop on Insider Attack and Cyber Security.

13. In addition to this work, I have cofounded two companies in cybersecurity. One company, StackSafe Inc. (formerly Revive Systems Inc.), was a provider of a virtualized preproduction staging environment that includes automated testing, analysis, and reporting for IT operations teams. I was with this company from its founding in 2005 until 2009. The second company, Allure Security Technologies (founded in 2010), develops deception-based solutions for detecting and mitigating the malicious cyber-insider threat, commercializing technology developed at Columbia through DHS and DARPA grants and a DARPA SBIR contract.

14. My curriculum vitae, which is appended to this declaration, details my background and technical qualifications. Although I am being compensated at my standard rate of $500/hour for my work on this declaration, the compensation in no way affects the statements in this declaration.

III. BACKGROUND OF THE ’181 PATENT

15. The ’181 patent discloses several embodiments relating to establishing secure communication links (*e.g.*, a link supporting encrypted communications) between devices connected over a network. The subject technology provides a “secure name,” and in some embodiments an “unsecure name,” associated with a remote device. In some embodiments, the “secure name” may be represented by a hyperlink or desktop icon, and allows a user to enable the secure communication link with just a “single click” or other minimal input to the device. (’181 patent 50:23-30, 56-61.)

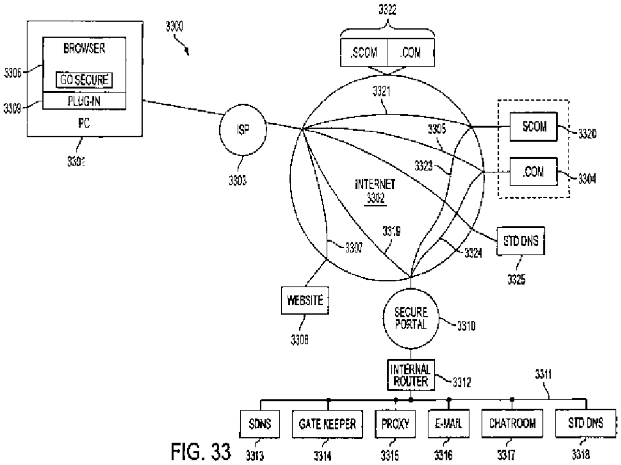


FIG. 33

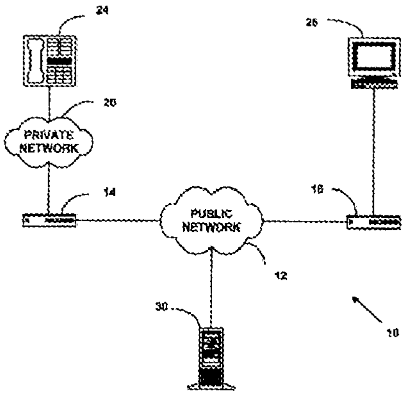
16. In one embodiment, depicted in Fig. 33 of the ’181 patent, reproduced above, computer 3301 may communicate conventionally with another computer 3304 over a non-secure communication link 3305 through a network 3302. A web page provided by computer 3304 to computer 3301 may contain a “Go Secure” hyperlink or icon for enabling a secure communication mode of communication between computer 3301 and computer 3304 over network 3302. (*Id.* at 50:54-61.) By selecting the displayed hyperlink or icon, the user enables a secure communication mode without having to enter user identification information, passwords, or encryption keys. (*Id.* at 49:66-50:3.) Accordingly, in one example, a software module 3309 located on computer 3301 may begin a process that establishes a secure communication link between computer 3301 and computer 3304. (*Id.* at 50:7-12.) The user may also enable the secure communication mode in other ways, such as, for example, by entering into the computer a command related to the “secure name” (*e.g.*, “go secure”). (*Id.* at 49:39-40.)

17. When a secure communication mode has been initiated, software module 3309 may query a secure name service (3313) for a secure network address of computer 3304. (*Id.* at 50:19-25.) The secure name service resolves secure names and facilitates establishing a secure communication link based on a secure name. In this respect, the secure name service cross-references secure names with corresponding network addresses for establishing secure communications with computer 3304. (*Id.* at 50:60-67.) The secure name service returns a network address for computer 3304, (*id.* at 51:26-29), and computer 3301 uses the network address and other provided resources to communicate securely with computer 3304, (*id.* at 51:44-46).

IV. BESER

18. Generally, *Beser* discloses a system for initiating a tunneling association that hides the identity of the originating and terminating ends of the tunneling association from other users. (*Beser* Abstract.) With reference to Fig. 1, reproduced below, *Beser* describes that a request is received at a first network device 14, the request including a unique identifier for a terminating telephony device 26. (*Id.* at 10:2-6, 22-23.)

FIG. 1



19. The trusted-third-party network device 30 is informed of the request, and associates the unique identifier with a public IP address of a second network device 16. (*Id.* at 11:26-32.) Then, private IP addresses for originating telephony device 24 and terminating telephony device 26 are negotiated and distributed to second network device 16 and first network device 14, respectively. (*Id.* at 11:59-12:54.) According to *Beser*, the tunneling association "hides the identity of the originating and terminating ends of the tunneling association from the other users of the public network." (*Id.* at 2:36-39.)

A. Claim 1

20. I understand that independent claim 1 recites "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device."

21. I understand that Requester generally alleges that "*Beser* shows security measures can be utilized which result in receiving, at a network address corresponding to the secure device, a message from a second device of the desire to securely communicate. For example, tunneling—a method of communicating securely—is taught in *Beser*." (*Id.* at 28.) I also understand that Requester cites Fig. 6 of *Beser* to support its analysis of this claim feature.

22. In my opinion, nothing in Fig. 6 of *Beser* shows "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." For example, "Request 112" cannot be the claimed "message" because this would require first network device 14 to be the claimed "first device" and originating telephony device 24 to be the claimed "second device." If this were the case, then *Beser* does not disclose sending a message over a secure communication link from the first device to the second device because the purported secure communication link (*i.e.*, *Beser*'s tunneling association, Req. at 29-31), is formed between originating telephony device 24 and terminating telephony device 26. It is not between first network device 14 and originating telephony device 24. "Inform 114" also cannot be the claimed message because it is not received "at a network address corresponding to the secure name associated with the first device." Requester alleges that the unique identifier of end-point devices (24, 26) is a "secure name" and that the "private IP addresses . . . assigned to the first and second network device (14, 16) and/or the end-point telephony device (24, 26)" is a network address corresponding to the secure name. But "Inform 114" is received by trusted-third-party network device 30 and not by any of end-point devices (24, 26) or first and second network devices (14, 16). The trusted third-party-network device 30 does not correspond to the purported secure name, the unique identifier. For the same reasons, "Negotiate 118" cannot be the claimed message because this also describes communications between one of network devices (14, 16) and trusted-third-party network device 30.

23. I also understand that claim 1 recites both a "first device" and a "second device" that include certain claimed features. For example, claim 1 recites: "receiving, at a network address corresponding to the secure name associated with the *first device*, a message from a *second device* of the desired to securely communicate with the *first device*" and "sending a message over a secure

communication link from the *first device* to the *second device*" (emphasis added). In my opinion, *Beser* does not disclose the recited first and second devices.

24. For example, end-point devices (24, 26) cannot be the "first device" and the "second device," because then *Beser* does not disclose "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." Of all the communications shown in Fig. 6 of *Beser* that Requester cites as purportedly disclosing the recited "message," none of these communications are between end-point device 24 and end-point device 26. (*See Beser* Fig. 6.) Moreover, *Beser* does not disclose that end-point device 24 receives a message from end-point device 26 of the desire to communicate securely with end-point device 24.

25. Likewise, first network device 14 and second network device 16 also cannot be the recited "first device" and "second device" because the purported secure communication link (*i.e.*, *Beser*'s tunneling association, Req. at 29-31), is formed between originating telephony device 24 and terminating telephony device 26, and not between first network device 14 and second network device 16.

26. I also understand that claim 1 recites "sending a message over a secure communication link from the first device to the second device." I understand that the Office and Requester allege that the tunneling association of *Beser* corresponds to the claimed "secure communication link" because "tunneling association hides the identity of the originating and terminating ends of the tunneling association from other users of a public network," and because the broadest reasonable interpretation of a secure communication link does not require encryption. (*See, e.g.*, Req. at 28.) I disagree for two reasons.

27. First, one skilled in the art at the time of the invention, after reading the '181 patent, would have understood that the claimed "secure communication link" requires the use of encryption. The '181 patent supports this interpretation by explaining that "[d]ata security is usually tackled using some form of data encryption." ('181 patent 1:50-57.) Indeed, encryption is described throughout the '181 patent as providing data security. (*See, e.g.*, *id.* 9:57-58; 11:5-7.) In the context of the claimed secure communication link, the '181 patent states that the secure communication link may be established without the need for a user to manually enter encryption keys, thus demonstrating that encryption is used in the secure communication link. (*See id.* at 50:1-3.)

28. *Beser*'s tunneling association between the originating and terminating devices is not a secure communication link as disclosed in the '181 patent because communication between these

devices is not encrypted. Instead, *Beser* discloses establishing a tunneling association that merely hides the identity of the originating and terminating ends of the tunneling association from other users of a public network. (*Beser* 2:36-40). In fact, *Beser* acknowledges encryption, but specifically teaches away from using it because, according to *Beser*, encryption may provide insufficient protection, may be infeasible to implement, and/or may create service problems due to computer-power limitations. (*Beser* 1:54-67.) One of ordinary skill in the art, when reading *Beser*, would understand that *Beser*'s tunneling association does not establish a secure communication link as disclosed in the '181 patent, but instead provides an alternative to establishing one.

29. Additionally, while the Office and Requester assert that *Beser* discloses using IPsec as "another method of securely communicating," (Req. at 28, citing *Beser* 1:54-56), this reference to IPsec appears in the "background" section of *Beser* and it not part of *Beser*'s tunneling association. Moreover, as I discussed above, the "background" section of *Beser* teaches away from using encryption in the configurations disclosed by *Beser*. (*Beser* 1:54-67.)

30. Second, even under Requester's incorrect construction of secure communication link that does not require encryption, *Beser*'s tunneling association is not a secure communication link. As discussed above, the tunneling association of *Beser* merely hides the identity of the originating and terminating ends from a hacker. (*Beser* 2:36-40.) But this tunneling does not secure those communications from eavesdropping once the originating and terminating ends have been discovered. For example, if a data packet sent over the tunneling association of *Beser* were to be intercepted, it could be examined, and the contents of the packet's data payload viewed. The '181 patent specifically distinguishes communications that incorporate "*data security*," and are thus "immune to eavesdropping," from communications that merely "prevent an eavesdropper from discovering that [a] terminal . . . is in communication with [another] terminal." ('181 patent 1:28-40.) *Beser* is directed to the latter; *i.e.*, to "establish a tunneling association that hides the identity of originating and terminating ends of the tunneling association from the other users of a public network," (*Beser* 2:36-39), and does not disclose the *data security* required to form a "*secure* communication link," as recited by claim 1.

B. Claim 2

31. I understand that independent claim 2 recites "a secure name service." I also understand that the Office and Requester allege that trusted-third-party network device 30 in *Beser* is the claimed "secure name service" because trusted-third-party network device 30 "may be a back-end service, domain name server, or the owner/manager of database or directory services." (Req. at 33,

quoting *Beser* 4:5-11.) I disagree. First, in my opinion, nothing in the above-quoted language of *Beser* shows a secure name service. Moreover, *Beser* does not disclose that trusted-third-party network device 30 is a secure name service, *i.e.*, that it facilitates establishing data security, much less facilitates establishing a secure communication link. For example, *Beser* discloses that its trusted-third-party network device "is connected to the public network," but omits any description of how the trusted-third-party network device is associated with any form of security. (*Beser* 4:1-2.)

32. I also understand that claim 2 recites "sending a message . . . using a secure communication link." In my opinion, *Beser* does not disclose this feature at least for the reasons I discussed above with regard to why the tunneling connection in *Beser* is not a secure communication link.

C. Claim 5

33. I understand that claim 5 recites "wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form." I also understand that the Office and Requester allege that "encryption can be used" because a background portion of *Beser* references IPsec. (Req. at 36.) In my opinion, this portion of *Beser* does not disclose the feature of claim 5 for two reasons.

34. First, this reference to IPsec is not part of the tunneling association of *Beser*. Additionally, as I discussed above with regard to claim 1, *Beser* discloses IPsec and other encryption techniques only to the extent that they should *not* be used in tunneled connections and VoIP applications, the technology with which *Beser* is primarily concerned.

35. Second, with respect to claim 2, from which claim 5 depends, the Office and Requester allege that a portion of *Beser* that recites "the first network device (14) has the following network addresses . . ." discloses the claimed "message containing the network address." (Req. at 35, citing *Beser* 21:38-43.) The cited portion of *Beser*, however, does not disclose receiving a message containing a network address, much less receiving a message in an encrypted form of any kind. In fact, nothing in *Beser* discloses encryption of a message containing the purported network address.

D. Claim 18

36. I understand that claim 18 recites "wherein the secure communication link is an authenticated link." I also understand that the Office and Requester cite to a part of *Beser* related to encryption and authentication of the purported secure name (*i.e.*, unique identifier) as corresponding to this feature. However, in my opinion, *Beser* does not disclose that encrypting or authenticating the

purported secure name (*i.e.*, the unique identifier) has anything to do with the purported secure communication link (*i.e.*, tunneling association).

E. Dependent Claim 23

37. I understand that dependent claim 23 recites that "the secure name of the second device is a secure, non-standard domain name." In my opinion, *Beser* does not disclose that the unique identifier for a device (*e.g.*, terminating telephony device 26) can be a "non-standard domain name." *Beser* is silent on the topic of standard/non-standard domain names.

F. Claim 24

38. I understand that independent claim 24 recites "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address." I also understand that the Office and Requester allege that the "unique identifier" (*i.e.*, the purported secure name) and the "public IP 58 address for the second network device 16" are associated because "the association of the secure name with the terminating device – is only possible because each device (including the originating device) has already requested and obtained registration of its secure name." (Req. at 46.) I disagree with this statement, however, because, the unique identifier of *Beser* (*i.e.*, the purported secure name) may be associated with the private IP addresses in any number of ways, including having been encoded into software, provided by an administrator, or transmitted by a device different than the purported first device.

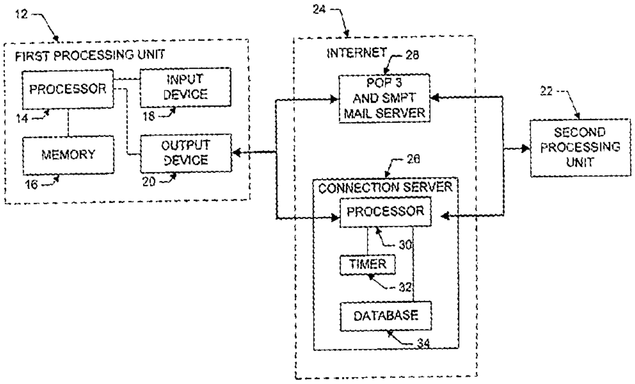
39. I also understand that claim 24 further recites "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device" and "sending a message securely from the first device to the second device." In my opinion, *Beser* does not disclose these features at least for the reasons discussed above regarding similar features of claim 1.

G. Claims 26, 28, and 29

40. Independent claims 26, 28, and 29 recite features similar to one or more of independent claims 1 and 2. My opinions expressed above regarding claims 1 and 2 also apply to claims 26, 28, and 29, to the extent these claims recite similar features.

V. MATTAWAY

41. *Mattaway* discloses two embodiments in which a first processing unit (12) sends a query for the network protocol address of a second processing unit (22) and establishes a communication link with the second processing unit upon receipt of the network protocol address. (*Mattaway* Abstract.)



42. In the first embodiment, *Mattaway* discloses a caller (*i.e.*, first processing unit 12) sending a packet, including an email address of a callee (*i.e.*, second processing unit 22) to a connection server (26) and the connection server returning the IP address of the callee. (*Mattaway* 18:48-64, explaining Fig. 16A.) In the second embodiment, *Mattaway* discloses the caller sending an email, including connection information for the caller, through a mail server (28) to the callee, and waiting for the callee to initiate a connection with the caller using the connection information. (*Mattaway* 7:63-9:15, 8:25-44.)

A. Claim 1

43. I understand that independent claim 1 recites "a first device associated with a secure name and an unsecured name." I also understand that Office and Requester allege that an email address stored on a server is a "secure name" because the server is "protected behind a 'firewall server 1522'" and Table 9 of *Mattaway* discloses an encrypted email address. (Req. at 70, citing *Mattaway* 17:44-48, 40:27.) I disagree for three reasons.

44. First, *Mattaway* does not disclose that the email address in Table 9 is associated with any particular device, much less the purported "callee's device" or any other device purportedly associated with the claimed "first device." *Mattaway* discloses that the data in Table 9 (including the purported secure name) is returned to a user (*i.e.*, the caller in the cited example) in response to a user "logging on for the first time" to a global server. (*Mattaway* Fig. 17A, 22:65-23:2.) The email address described in Table 9 is not referenced in any other portion of *Mattaway*, and *Mattaway* is completely silent as to the function of the referenced email address and whether it could be associated with a device. In fact, *Mattaway* does not disclose encrypting an email address associated with a device.

45. Second, the firewall of *Mattaway* does not protect email addresses as contended by the Office and Requester. In fact, if a callee's email address were to be stored on a server behind the firewall (*e.g.*, the global server 1500), that email address would already be known to the caller before

the caller connects to the server. For example, Figure 16A, cited in the Request at pages 70-71, teaches that an email address is received at the global server, from a caller device, as part of a <CONNECT REQ> packet. Similarly, in another example cited in the Request, an email address is sent from a caller to the callee, through a mail server, and the caller waits for a response email. (*Mattaway* 7:62-8:35.) In both examples, the email address purported to be a "secure name" originates from a different location (*i.e.*, a caller device) than what the Office and Requester point to as providing the purported security to transform the email address into a "secure name" (*i.e.*, the global server).

46. Third, nothing in *Mattaway* discloses or suggests that an email address received by the global server of *Mattaway*, or used by the caller or callee, is a "secure name," much less associated with any security whatsoever. In fact, the terms "secure" or "security," or the like, are completely absent from *Mattaway*.

47. I understand that claim 1 further recites "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[ ] to securely communicate with the first device." I also understand that the Office and Requester assert that two different embodiments in *Mattaway* disclose this feature. (Req. at 70-71, citing *Mattaway* Fig. 16A, 8:25-44.) I disagree because *Mattaway* does not disclose a "message . . . of the desire[ ] to securely communicate." The Office and Requester conclude that Figure 16A of *Mattaway* discloses an "intent to securely communicate," but do not point to any explicit passage or provide any reasoning as to how the feature might be inherent, and, in my opinion, *Mattaway* does not disclose such a feature.

B. Claim 2

48. I understand that independent claim 2 recites "from a first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device." I disagree with the Office's and Requester's assertion that the connection server 26 is a "secure name service" because the purported secure name service (*i.e.*, connection server 26) does not store a "secure name" for the callee's device, as proposed by the Office and Requester. (*See* Req. at 74.) Moreover, nothing in *Mattaway* indicates that the email address identified in Table 9 is associated with any particular device.

49. I also understand that claim 2 recites "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication

link." In my opinion, *Mattaway* does not disclose this feature for reasons similar to those that I discuss above with regard to claim 1.

C. Claim 7

50. I understand that claim 7 recites "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." As I understand it, the Office and Requester point to one sentence in *Mattaway* that states one of two example protocols may be used in establishing communication with a callee processing unit. (Req. at 75, citing *Mattaway* 6:37-45.) Discussing these exemplary protocols, however, does not disclose a device "capable of supporting a *secure communication link* <u>*as well as*</u> *a non-secure communication link*," or "establishing a non-secure communication link with the second device *when needed*," as recited by claim 7. Besides, *Mattaway* does not disclose how the named protocols could be used to produce the claimed feature.

D. Claim 13

51. I understand that claim 13 recites that "the receiving and sending of messages through the secure communication link includes multiple sessions." The Requester and the Office contend that the "point-to-point Internet communications with the callee" that arise from a single call correspond to the claimed secure communication link. (Req. at 74.) But *Mattaway* discloses that each call receives a new session. (*Mattaway* 6:24-36.) Thus, in my opinion, *Mattaway* discloses that the receiving and sending of messages during a call (the purported secure communication link) includes only one session, not multiple sessions.

E. Claim 24

52. I understand that independent claim 24 recites "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address." I also understand that Office and Requester assert that *Mattaway* discloses this feature because *Mattaway* discloses "the first processing unit 12 automatically transmits its associated E-mail address . . . to the connection server 26." (Req. at 80-81, quoting *Mattaway* 6:60-65.) I disagree. As I discuss above regarding independent claim 1, *Mattaway* does not disclose or suggest a "secure name." Moreover, in my opinion, automatically transmitting an email address is not the same as "requesting and obtaining registration" of the email address, much less of a "secure name."

53. I understand that claim 24 further recites "receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device" and "sending a message securely from the first device to the second device." In my opinion, *Mattaway* does not disclose these features at least for the reasons discussed above regarding similar features of claim 1.

54. I also understand that claim 24 further recites "sending a message securely from the first device to the second device." I understand that the Office and Requester allege that *Mattaway* discloses feature by stating that a "WebPhone application enables the parties to converse in real-time, telephone quality, encrypted audio communication." (Req. at 83, quoting *Mattaway* 25:32-34.) I disagree because this passage discloses nothing about whether, much less how, a message may be sent securely. Thus, in my opinion, this passage does not disclose "sending a message securely from the first device to the second device."

F. Claims 26, 28, and 29

55. Independent claims 26, 28, and 29 recite features similar to one or more of independent claims 1 and 2. My opinions expressed above regarding claims 1 and 2 also apply to claims 26, 28, and 29, to the extent these claims recite similar features.

VI. MATTAWAY IN VIEW OF BESER

A. Claim 18

56. I understand that claim 18 recites "wherein the secure communication link is an authenticated link." I also understand that the Office and Requester point to a passage in *Beser* related to authenticating the purported secure name (*i.e.*, the user identifier), and then allege that a person skilled in the art would have recognized using that form of authenticating in the purported secure communication link of *Mattaway*. (Req. at 98.) I disagree because *Beser* does not disclose that the encrypting or authenticating of the purported secure name (*i.e.*, the unique identifier) has anything to do with the purported secure communication link (*i.e.*, tunneling association) of *Beser*, and therefore it cannot be combined with the purported secure communication link of *Mattaway*. Thus, the two features that the Requester wishes to combine are applicable to different mechanisms within their respective references.

VII. LENDENMANN

57. Generally, *Lendenmann* discloses a distributed computing environment ("DCE"), which "is a layer of services that allows distributed applications to communicate with a collection of computers, operating systems, and networks." (*Lendenmann* 7.) As illustrated in Figure 3,

Lendenmann's DCE may include several different components, including security services, time services, and directory services. (*Id.* at 8.)

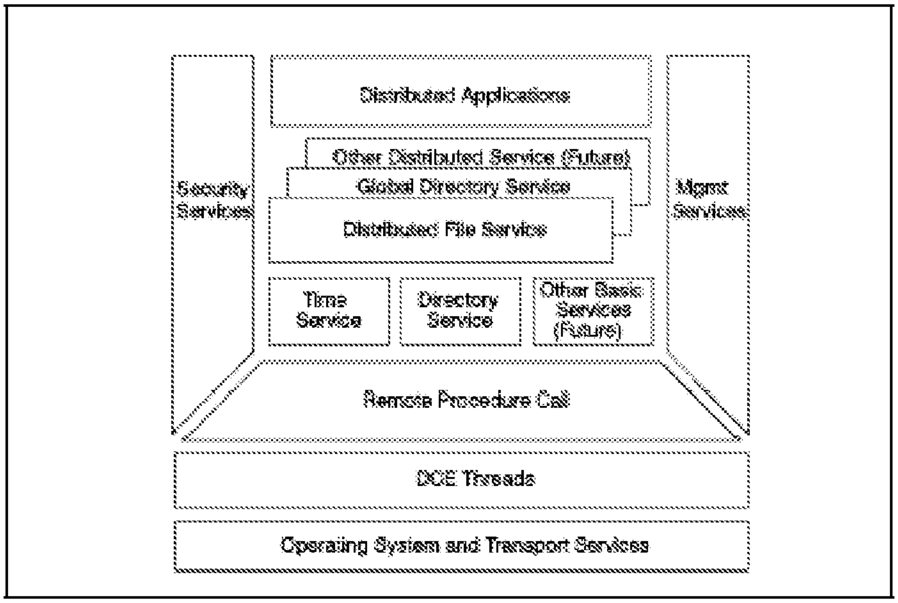


Figure 3. DCE Architecture

(*Id.*) It further discloses that a collection of machines, operating systems, and networks managed by a single set of DCE services constitutes a "DCE cell." (*Id.*) At a minimum, a cell must contain a Security Server, a Cell Directory Server ("CDS"), and Distributed Time Servers. (*Id.* at 9.) These separate components provide different services for establishing remote procedure calls ("RPCs") between clients and servers.

58. RPCs between clients and servers may or may not employ security features, such as authentication and encryption. (*See, e.g.*, *id.* at 192.) Whether an RPC utilizes security features lies completely within the discretion of the client. (*Id.* at 71, 192.) A client may select the desired security level only after obtaining a binding handle containing a network address for a server, as the server must also be able to support the designated security features. (*Id.* at 71, 207-08.) For interoperability purposes, *Lendenmann*'s DCE supports two naming schemes for organizing server network addresses: X.500 and DNS. (*Id.* at 21.) These binding handles, available from several different sources, also contain various other information necessary for the client to connect to a server during the RPC process, including, for example, object UUIDs, protocol sequences, and endpoints. (*Id.* at 182-84.)

59. To locate a server to remotely provide services or applications over the DCE, a client searches for servers during the "binding" process. (*Id.* at 182.) A client must first decide on a binding method, and *Lendenmann* describes three alternatives: automatic, implicit, or explicit

binding. (*Id.* at 180.) A client then must locate servers, for which *Lendenmann* also describes several alternatives: searching files, environment variables, or the CDS; or simply hard-coding a network address into an application. (*Id.* at 182.) A client then obtains binding handles from various possible sources, such as the server RPC runtime, the server host DCE daemon, the CDS, or the client RPC runtime. (*Id.* at 182-83.) These binding handles each identify a server to the client. (*Id.* at 182.) Because *Lendenmann*'s clients search for compatible servers that "handle[] the interface that the client is interested in," (*id.*), a client might receive binding handles for several compatible servers. (*Id.* at 185, describing the process of obtaining binding handles from the CDS.) Upon choosing an appropriate binding handle, the client may select supported security features, call the server, and establish an RPC. (*See id.* at 207-08, "Putting It All Together.")

A. Claim 1

60. I understand that independent claim 1 recites "a first device associated with a secure name and an unsecured name," and that the Office and Requester assert that *Lendenmann* discloses this feature because of the "distinction between the X.500 and DNS naming conventions," namely that X.500 is secure, while DNS is unsecured. (OA at 7; Req. at 102, identifying X.500 names as secure names; *id.* at 105-06.) I disagree because *Lendenmann* simply presents X.500 and DNS as two alternative DCE-compatible general naming schemes for organizing network addresses: "X.500 is an emerging global directory service standard, but the Internet domain name system (DNS) is an established industry standard. For interoperability purposes, GDS supports both X.500 and DNS transparently." (*Lendenmann* 21.)

61. I understand that the Requester highlights two differences between the DNS and X.500 schemes, but it fails to explain how these differences suffice to make X.500 "secure" and DNS "unsecured." (Req. at 105.) The Requester first asserts that Figure 10, reproduced below, reveals a secure/unsecure distinction between X.500 and DNS.

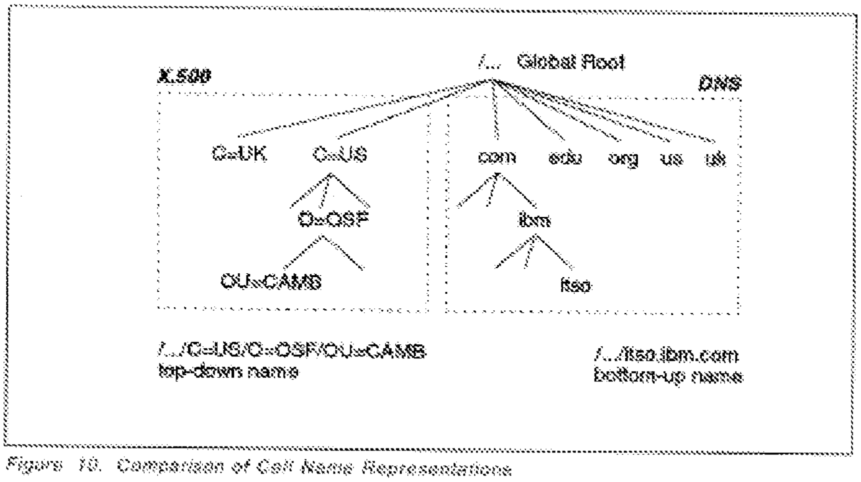


Figure 10. Comparison of Cell Name Representations

Figure 10 shows a comparison of the DNS hierarchical tree structure and the X.500 CDS representation. X.500 picks the names in a top-down order, while DNS does it in bottom-up order.

(Req. at 106; *Lendenmann* 24.) As *Lendenmann* explains in the caption, Figure 10 illustrates an organizational difference between X.500 and DNS. (*Id.*) X.500 organizes names in a "top-down" order, while DNS organizes names in a "bottom-up" order. (*Id.*) But the Figure 10 does not indicate a secure/unsecure distinction between X.500 and DNS.

62. I understand that the Request further contends that DNS is unsecured because it has "global addressing and routing," whereas X.500 is secure because it is an "internal naming convention" implemented with a service (GDS) that "can store any kind of object." (Req. at 105, quoting *Lendenmann* 23.) I disagree because *Lendenmann* specifically requires a "global network routing mechanism" to access foreign cells on the Internet, "[t]he only well-established, multi-vendor-supported global network today." (*Lendenmann* 23.) *Lendenmann*'s distributed computing environment specifically uses GDS (and thereby X.500) for storing "Internet addresses." (*Lendenmann* 23.) In either X.500 or DNS, "access to the foreign cell *is established over the Internet in both cases*." (*Id.*) Thus, *Lendenmann* illustrates that in its disclosed distributed computing environment, X.500 and DNS perform the same functions, and are simply alternative DCE-compatible naming schemes. (*Id.* at 21-23)

63. Regardless of whether a user attempts to obtain a network address based on an X.500 name or a DNS name, a user cannot access the CDS at all unless the user is first cleared by the Security Service. (*Lendenmann* 34.) The Security Service weeds out unauthorized users without regard to the naming scheme employed by each user (X.500 or DNS). (*Lendenmann* 34.)

Lendenmann does not provide for any second layer of protection in its CDS directory service based on naming scheme or otherwise.

64. Furthermore, in my opinion, *Lendenmann* does not teach that all names retrievable from a CDS are "secure" names. For example, *Lendenmann* does not specify any security-related procedures or results that stem from employing an X.500 name or a DNS name in establishing RPCs—which purportedly corresponds the "secure communication link" of claim 1. *Lendenmann* explains that implementation of any security features during RPCs lies within the complete discretion of the user-client, regardless of the naming convention employed. (*Lendenmann* 71, "RPC clients *may choose* a security level they want to use. Of course, the level they choose must match a level supported by the server," emphasis added.) *Lendenmann* goes on to explain that "[w]hen a client establishes authenticated RPC, it *can specify* the level of protection to be applied to its communication with the server," including "None." (*Lendenmann* 192, emphasis added.) Thus, in my opinion, any security-related aspects of *Lendenmann* are independent of the decision to use X.500 names or DNS names.

65. I understand that independent claim 1 additionally recites "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device." As I explain above, *Lendenmann* does not teach that X.500 names are "secure" in any fashion. Regardless, in my opinion, even if one were to incorrectly assume that an X.500 name corresponds to a "secure name," *Lendenmann* fails to describe receiving any message at a network address corresponding to an X.500 name instead of a DNS name. The Requester points to *Lendenmann*'s RPC runtime call to a server as the "message" of claim 1, in which *Lendenmann* a client's RPC runtime may search for addresses to include in its binding information to send to a server. (Req. at 107-08; *Lendenmann* 182, 186-87.) But *Lendenmann* does not teach including X.500 addresses in the binding information, much less any security-related consequences of utilizing X.500 names versus DNS names. (*See, e.g.*, *id.* at 190, describing the process of "1. Looking up a binding in CDS.")

B. Claim 2

66. I understand that independent claim 2 recites, among other things, "a secure name service." I understand that the Office and Requester contend that the CDS is a secure name service because the DCE's Security Service controls access to the CDS by requiring authentication and authorization before the CDS completes any name-service operations. (OA at 7; Req. at 112-13.) I disagree because the CDS has no bearing on whether the communications for which it provides

network addresses are secure or not. One of ordinary skill in the art would have understand that a "secure name service" in the context of the '181 patent is a service that both resolves a name into a network address and further supports establishing a secure communication link. The CDS's role, however, is limited to providing binding information for RPC. (*Lendenmann* 207-08, describing the overall RPC process.) The security features for RPC, if any, are incorporated only after the client has finished obtaining the necessary binding information: "After the client has the binding handle, it can add to it the desired security level for the RPC calls. Then it issues an RPC . . . ." (*Id.* at 208.)

67. In my opinion, because the CDS has no bearing on whether the communications for which it provides network addresses are secure, the CDS performs no functions beyond those that the '181 patent recognizes and distinguishes as being conventional name services. For example, the conventional name service described in the '181 patent, similar to the CDS, does nothing more than return server-identifying information, such as an IP or network address. (*See, e.g.*, '181 patent 38:54-56.) My understanding is that the '181 patent distinguishes its inventive name services, such as the "secure name service" recited in claim 2, as those that do not simply return an IP address but also further support establishing a secure communication link, such as by "automatically set[ting] up a virtual private network between the target node and the user." (*Id.* at 39:30-31.) As the '181 patent teaches, whether such security features are ultimately employed depends precisely on whether the name of the target server is "secure" or not, unlike with *Lendenmann*'s CDS and RPC procedures, as discussed above. (*Id.* at 39:53-40:14.) Thus, *Lendenmann*'s CDS does not disclose a "secure name service," as recited in claim 2.

68. I understand independent claim 2 further recites, "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device." As I understand them, the Office and Requester contend that a client's requesting a network address for a server during the "binding" process corresponds to the "message" recited in claim 1. (OA at 7; Req. at 112.) I disagree. *Lendenmann*'s binding process does not involve "requesting a network address" associated with any server name at all, let alone a "secure" name. *Lendenmann* generically describes that its CDS may return a network address upon receiving a name, (*Lendenmann* 21), but this does not apply to interactions between a client and the CDS during the binding process. (*Id.* at 33, explaining that "[t]he RPC client uses the Name Service Interface (NSI) API to get binding information from the CDS"; *id.* at 186, discussing the NSI.) Rather, within the binding process, *Lendenmann* only discloses clients locating services based on criteria *other than server names* during the binding process. (*See, e.g.*, *id.* at 186-87, NSI and

"Searching The Namespace.") For example, as *Lendenmann* explains and the Request quotes, "[a] client can find a server by asking the CDS for the location of *a server that handles the interface that the client is interested in*," not the location of a server having any particular name. (*Lendenmann* 182.) Similarly, *Lendenmann* discloses that "[w]hen a client wants to connect to a server, it needs to find a compatible server" rather than one associated with any particular server name. (*Lendenmann* 185.) *Lendenmann*'s RPCs, appropriately described as "function calls," are designed to find servers based on functional criteria to provide services (*e.g.*, applications) from remote locations in the distributed computing environment—not to find servers associated with a particular server name. (*Lendenmann* 172.)

69. Rather than the client in *Lendenmann* providing a name to a name service to identify a server, "[b]inding information includes a set of data that *identifies a server to a client*." (*Lendenmann* 182, emphasis added.) Therefore, "when the client looks for binding handles, it might obtain handles to *several compatible servers*," *i.e.*, not one associated with any particular name. (*Lendenmann* 185, emphasis added.) The NSI performs these server-identification functions for the client, and *Lendenmann* teaches that the NSI provides mechanisms for "search[ing] server entries for a compatible server." (*Lendenmann* 186.) The existence of these mechanisms to search among various compatible servers or to obtain binding information as a means of identifying a server to the client indicate to one of ordinary skill in the art that *Lendenmann* does not disclose a client providing a server name to look up a network address, because the identity of the desired server would have already been known from the server name.

70. I understand that independent claim 2 recites, "sending a message to the network address associated with the secure name of the second device using a secure communication link." If one incorrectly assumes that *Lendenmann* discloses "secure" names, it is my opinion that *Lendenmann* does not disclose that its RPC-related security features—the purported "secure communication link"—have anything to do with the purported secure (X.500) or unsecured (DNS) names. (Req. at 114-15, merely listing various protection levels disclosed in *Lendenmann.*) Even if the use of X.500 names is involved in these RPC features (which it is not), it is not necessarily the case that *Lendenmann*'s system would utilize X.500 names during security-enhanced communications. *Lendenmann*'s DNS and X.500 names are security-independent and are provided merely as alternative DCE-compatible naming schemes "[f]or interoperability purposes." (*Lendenmann* 21, 71, 192.) *Lendenmann's* security features are left in the complete discretion of its user-clients, as I explained above.

C. Dependent Claims 5 and 6

71. I understand that dependent claims 5 and 6 depend from claim 2 and specify that the "receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form" and that it involves "decrypting the message," respectively.

72. I understand that the Office and Requester contend that *Lendenmann* discloses these features because it purportedly describes querying the CDS for binding information via encrypted communications and subsequently decrypting the CDS's response. (OA at 7; Req. at 117-21.) In my opinion, however, *Lendenmann* discloses a far different role for the CDS in establishing RPCs than the Requester's effort to imply that the client and the CDS might themselves communicate via encrypted RPC. Nowhere does *Lendenmann* disclose that utilizing a CDS in establishing an RPC between a client and a server might first involve establishing an encrypted RPC between the client and the CDS. (*See Lendenmann* 173, "This chapter [10] discusses all components involved in the execution of an RPC, including CDS and Security Services"; *see also id.* at 33, "CDS Lookup.") *Lendenmann* provides some security measures to protect a client's accessing of information in the CDS, but these measures notably exclude encryption: "The CDS, as any other DCE service, is integrated into the security service. The CDS server only completes an operation over the clearinghouse if the user is *authenticated and authorized* by the Security Service." (*Lendenmann* 34.)

D. Dependent Claim 21

73. I understand that dependent claim 21 depends from claim 2 and recites "providing an unsecured name associated with the device." *Lendenmann* does not disclose that its CDS may provide both a *network address* corresponding to an X.500 name (a purportedly secure name) *and a DNS name itself* (a purported unsecured name) to the claimed "first device." *Lendenmann* explains that X.500 and DNS names are used in the alternative to each other, not that they are both used simultaneously. (*Lendenmann* 24.)

E. Independent Claim 24 and Dependent Claim 25

74. I understand that in their analysis of independent claim 24 and dependent claim 25, the Office and the Requester, having earlier asserted with respect to claims 1 and 2 that X.500 names are "secure" while DNS names are "unsecured," now change their position by asserting that *all* names stored within the CDS are "secure," whether X.500 or DNS. (OA at 7; Req. at 134.) As its basis for this change in position, Requester explains that the Security Service must authenticate and

authorize a user before the CDS completes any name-service operations. (Req. at 134, citing *Lendenmann* 23.) This assertion that *all* names within the CDS namespace are "secure" is contrary to the clear teachings of *Lendenmann*, which expressly teaches that implementation of any security features during RPCs lies within the complete discretion of the user-client. (*Lendenmann* 71, "RPC clients *may choose* a security level they want to use. Of course, the level they choose must match a level supported by the server," emphasis added.) As I mentioned above, "[w]hen a client establishes authenticated RPC, it *can specify* the level of protection to be applied to its communication with the server," including "None." (*Lendenmann* 192, emphasis added; *see also id.* at 207-08, "After the client has the binding handle, it can add to it the desired security level for the RPC calls. Then it issues an RPC . . . .") Thus, the names stored in the CDS are security-independent and there is no basis for calling them "secure" or "unsecured."

F. Independent Claim 26 and Dependent Claim 27

75. I understand that claim 26 and claim 27 depending from it contain the feature "requesting and obtaining registration of a secure name associated with the first device, *wherein a unique network address corresponds to the secure name associated with the first device*," (emphasis added). Requester points to a portion of *Lendenmann* that generically describes "registering servers in the namespace," but neither this passage nor any other in *Lendenmann* discloses that a server may be registered with an additional "unique network address" corresponding to another name, much less a "secure" name. (Req. at 142, citing *Lendenmann* 203.) But, in my opinion, nothing in *Lendenmann* requires that purportedly "secure" X.500 names must *necessarily* correspond to unique network addresses.

G. Independent Claims 2, 26, 28, and 29

76. It is my opinion that independent claims 2, 26, 28, and 29 recite features similar to one or more features of independent claims 1. My opinions expressed above regarding claims 1 also apply to claims 2, 26, 28, and 29, to the extent these claims recite similar features.

VIII. PROVINO

77. Generally, *Provino* discloses a system for connecting an external device to a device on a virtual private network via a secure tunnel between the external device and a firewall associated with the virtual private network. (*Provino* Abstract.) Referring to FIG. 1 of *Provino*, reproduced below, when an operator at a device 12(m) wishes to connect to a device 13 on the Internet, the operator inputs a human-readable address of the device 13, causing the device 12(m) to send a message to a name server 17 requesting the corresponding Internet address of the device 12(m). (*Id.*

at 8:14-40, 11:5-11.) The name server 17 does not have the addresses of the devices 31 on the virtual private network 15, except for the address of the firewall 30 of the virtual private network 15. In response to a request for the Internet address of a device 31 on the virtual private network 15, the name server returns the Internet address of the firewall 30. (*Id.* at 10:45-55, 11:11-16.)

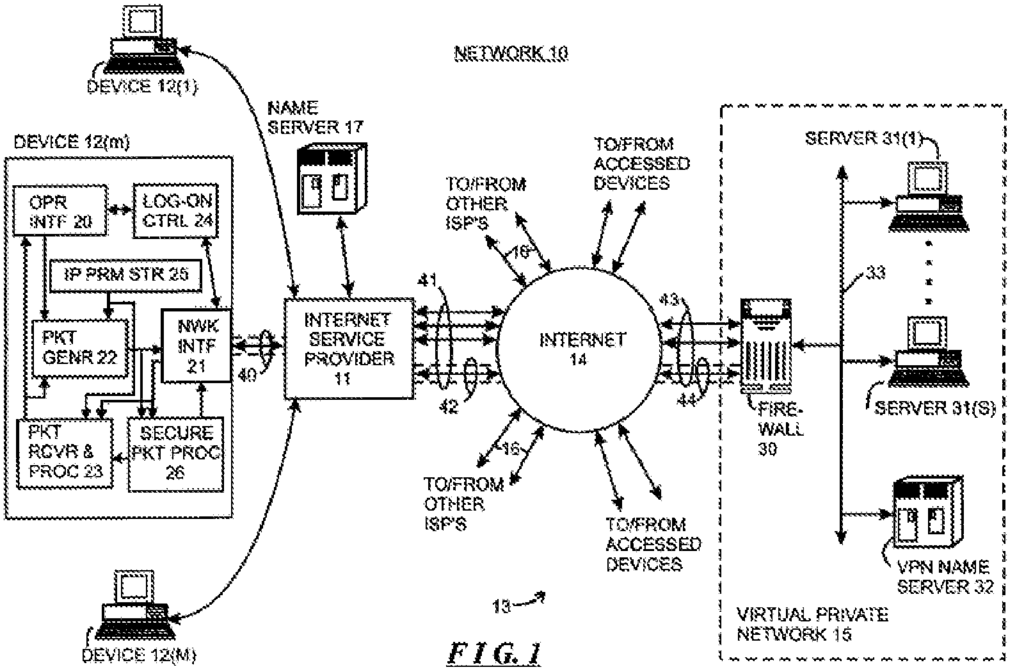


FIG. 1

78. The device 12(m) initiates establishment of a secure tunnel with the firewall 30. (*Id.* at 9:32-56, 10:56-58, 11:13-16.) Further, the firewall 30 provides the device 12(m) with the identification of a second name server 32 inside the virtual private network 15. (*Id.* at 10:62-63.) The device 12(m) sends, over the secure tunnel, a message to the second name server 32 requesting the Internet address of the device 31 on the virtual private network 31 corresponding to the human-readable address of the device 31. (*Id.* at 10:62-67, 11:17-26.) Thereafter, the device 12(m) is able to communicate with the device 31 on the virtual private network 15 via the secure tunnel.

A. Independent Claim 1

79. I understand that independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." The Requester contends that "Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, *i.e.*, the Domain name stored in the VPN Name Server 32, and one being an unsecured name, *i.e.*, the Domain name stored in Name Server 17 at ISP 11." (Req. at 168.) Requester quotes *Provino* at 10:45-52 to support its position, but that passage actually states that name server 17 does not contain *any* name associated with servers 31(S):

"nameserver 17 is not provided with integer Internet addresses for servers 31(S) and other devices which are in the virtual private network 15." (*Provino* 10:48-51.) Thus, "the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(S) which is to be accessed from that nameserver 17." (*Provino* 10:52-55.) Network addresses related to firewall 30 may be contained in name server 17, but not the network addresses for servers 31(S). (*Provino* 10:51-52.)

80. I understand that claim 1 calls for a "secure name" in two places: "a first device associated with a *secure name* and an unsecured name" and "receiving, at a network address corresponding to the *secure name* associated with the first device." In my opinion, however, *Provino* does not disclose any "secure names." One of ordinary skill in the art would understand that "secure names" in the context of the '181 patent are those names used to communicate securely that are resolved by a secure name service (*i.e.*, a service that both resolves a name into a network address and further supports establishing a secure communication link). The name servers in *Provino*, on the other hand, are conventional name servers of the type distinguished in the '181 patent and do not qualify as a "secure name service" that can resolve "secure names."

81. For example, the '181 patent discloses that a conventional domain name service system merely returns an IP address corresponding to a domain name. For example, in one embodiment, the '181 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('181 patent 38:54-59; *see also* '181 patent 38:61-39:13.)

82. In my opinion, the name servers 17 and 32 of *Provino* are similar to the conventional domain name systems described by the '181 patent in that they return a requested Internet address of a device corresponding to the human-readable address of that device, such as the requested IP address corresponding to a domain name like "Yahoo.com." (*Compare Provino* 8:48-51 *with* '181 patent 38:54-59.) In particular, *Provino* discloses that name server 17 "can resolve the human-readable domain names to provide the appropriate Internet address for the destination referred to in the respective human-readable name." (*Provino* 7:40-43.) It resolves names for devices located outside the firewall 30 and for the name of the firewall itself. Name server 32 operates in a similar manner except it resolves addresses for servers 31(s) behind firewall 30. (*Provino* 9:2-5, stating that name server 32 merely "serves to resolve human-readable Internet addresses for servers 31(s)

internal to the virtual private network 15 to respective integer Internet addresses.") In both instances, name servers 17 and 32 operate in the conventional manner described and distinguished in the '181 patent specification in that they merely resolve a requested human-readable address but do not resolve "secure names" or support establishing a secure communication link as in the case of a secure name service. The '181 patent recognizes that such conventional domain name services suffer from certain drawbacks and thus discloses embodiments that address them, including embodiments with secure name services that resolve "secure names" as recited in claim 1. (*See, e.g.*, '181 patent 39:23-25.)

83. It is also my understanding that the claims require the "first device" to be "associated with a secure name and an unsecured name." Initially, since *Provino* does not disclose the claimed "first device," for the reasons I provided above, it is my opinion that *Provino* does not disclose the following features, which also involve the undisclosed "first device"

- receiving, at a network address corresponding to the secure name associated with the *first device*, a message from a second device of the desired to securely communicate with the *first device*; and
- sending a message over a secure communication link from the *first device* to the second device.

84. I understand that the Requester contends that *Provino* discloses the claimed "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device" because:

> Provino discloses that the establishment of the secure communication link between devices can be initiated by a first device (device 12 (m)) that is external to the virtual private network 15. In this manner, "the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. Provino at 9:46-52.

(Req. at 171.)

85. In my opinion, Requester is incorrect because device 12(m) is not associated with a secure name. (Requester never alleges that it is, instead contending only that server 31(S) is associated with a secure name. (*See* Req. at 168.) Device 12(m) cannot receive anything "at a network address corresponding to the secure name associated with the first device" because it has no secure name associated with it in the first place.

86. Even if one were to assume that server 31(S) had an associated secure address as purported by Requester—the Requester would still be incorrect. As Requester acknowledges, it is

the *firewall 30* that receives messages from device 12(m) to create a tunnel, not server 31(S). In fact, server 31(S) does not receive the purported request "requesting establishment of a secure tunnel between the device 12(m) and firewall 30," and Requester never contends that it does. (*See* Req. at 171.)

B. Independent Claims 2, 26, 28, and 29

87. I understand that independent claims 2, 26, 28, and 29 recite features similar to one or more features of independent claim 1. My opinions expressed above regarding claims 1 also apply to claims 2, 26, 28, and 29, to the extent these claims recite similar features.

IX. H.323

88. *H.323* describes the components of an H.323 system, which provides multimedia communications services over Packet Based Networks (PBN). (*H.323* i.) Various remote endpoints may communicate over the H.323 system via point-to-point calling. (*Id.* at 4-5, "3.7 call.") Endpoints may include a terminal, a gateway, or a multipoint control unit (MCU). (*Id.* at 5, "3.14 endpoint.") Other non-callable entities include gatekeepers and multipoint conferences. (*Id.*, "3.9 callable.") *H.323* explains that each entity has at least one network address, and that endpoints may additionally be associated with one or more alias addresses. (*Id.* at 33.) An alias address may represent either an endpoint itself or a service (*e.g.*, a conference) hosted by an endpoint. (*Id.*) An access token may shield an endpoint's alias address and transport address (*i.e.*, network address plus a TSAP identifier) from another endpoint during the calling process. (*Id.* at 38; *id.* at 8, "3.42 transport address.")

89. When establishing a call, one endpoint may call another via a gatekeeper. (*Id.* at 34.) Endpoints must register with a gatekeeper in order to participate in gatekeeper functions. (*Id.* at 37.) For example, gatekeepers may translate alias addresses to transport addresses, although any potential directory services are undefined. (*Id.* at 27.) Other functions include admission control, bandwidth control, and zone management, among others. (*Id.* at 33.) Using access tokens requires endpoints to route communications through a gatekeeper. (*Id.* at 38.) Endpoints may also call each other directly, particularly when no gatekeeper exists in an H.323 system. (*See, e.g., id.* at 27.)

90. Establishing a call proceeds through the process of "call signalling." (*Id.* at 33.) The call procedures occur as follows: (A) call setup, (B) initial communication and capability exchange, (C) establishment of audiovisual communication, (D) call services, and (E) call termination. (*Id.* at 41.)

A. Claim 1

91. I understand that independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." It is my understanding that the Office and Requester assert that alias addresses protected by "access tokens" correspond to secure names. (OA at 11; Req. at 209.) They also assert that an endpoint having an access-token-protected alias (*i.e.*, an alleged "first device") could additionally have an alias corresponding to a gatekeeper entity, or an alias corresponding to a conference hosted by the endpoint, with either allegedly corresponding to an "unsecured name." (OA at 11; Req. at 210-11.) I also understand that the Office and Requester allege that a uniform resource locator (URL) for a gatekeeper corresponds to the "unsecured name." (OA at 11; Req. at 210-11.) They further assert that if the endpoint having an access-token-protected alias is a gateway, a first Switched Circuit Network (SCN) endpoint obtaining access to the PBN via the gateway might have an alleged "unsecured name," and that a second SCN endpoint obtaining access to the PBN via the gateway might have a "secure name." (Req. at 212-13.) I disagree.

92. The Office and Requester's position that the URL for a gatekeeper corresponds to the unsecured name recited in independent claim 1 is incorrect because *H.225* discloses that the URL is for the gatekeeper. (*H.225* 141.) Thus, in my opinion, the URL (*e.g.*, the alleged unsecure name) is associated with the gatekeeper rather than with the called *H.323* endpoint, the purported first device.

93. I understand the Office and Requester also contend that if the *H.323* endpoint is a Gateway, (*see* Req. at 211), a first SCN endpoint that is obtaining access to the PBN through the Gateway has an unsecure name. (Req. at 212-13.) The Office and Requester point to pages 4-6 of *H.323* to support its argument. (Req. at 212-13.) I disagree. This passage of *H.323* does not discuss any name for the first SCN endpoint, much less explain that it has an unsecure name. (*H.323* 4-6.) The passage just states, in relevant part, "[i]n case of interworking with some SCN endpoints via a Gateway, all the channels terminate at the Gateway." (*Id.*)

94. Furthermore, the *H.323* references do not disclose that when an access token is used to protect an alias address of a called endpoint (*i.e.*, the purported secure name), the called endpoint would also have a different alias address that is not protected by the access token (*i.e.*, the purported unsecure name). The combined *H.323* references do not show the called endpoint having an alias address protected by an access token (*i.e.*, a purported secure name) as well as another alias address not protected by an access token (*i.e.*, a purported unsecured name).

95. Furthermore, an alias address protected by an access token or the access token itself does not correspond to the "secure name" recited in claim 1. The Office and Requester point to page

38 of *H.323* to support the notion that *H.323* discloses a secure name. However, this passage does not discuss security at all but explains that access tokens "provide privacy by shielding an endpoint's Transport Address and Alias address information from a calling party." (*H.323* 38.) In my opinion, privacy and security are distinct features, and providing privacy for an alias address would not necessarily make the alias address a secure name.

96. The second SCN endpoint cannot correspond to the "secure name" for the same reasons that the first SCN endpoint cannot.

97. I understand that independent claim 1 also recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device."

98. The Office and Requester contend that an alias address protected by an access token or the access token itself corresponds to the "secure name" recited in claim 1. (*See* Req. at 214.) But, in my opinion, *H.323* does not describe receiving any message at a network address corresponding to an access-token-protected alias *rather than* to a second, "unsecured" alias. *H.323* explains that its access tokens merely "shield[] an endpoint's Transport Address and Alias Address," and therefore *H.323* does not disclose any "message . . . of the desired to securely communicate." (*H.323* 38.) In my opinion, merely shielding the endpoints of communications does "not secure those communications from eavesdropping."

99. It is my opinion that *H.235* also fails to disclose receiving any "message . . . of the desire[] to securely communicate" at a network address corresponding to any access-token-protected alias address (*i.e.*, alleged secure name). Without identifying any message in particular, I understand the Requester points to at least five sections of *H.235* as disclosing these features. (Req. at 214.) Each passage fails to support the position.

100. In my opinion, the *H.235* token feature does not disclose the above "message" features of claim 1. (*See* Req. at 214-15.) Any messages associated with the *H.235* token feature serve to "obscure or hide destination addressing information," not to communicate any desire to securely communicate. (*H.235* 28-29.) As I have already stated, obscuring or hiding the endpoints of communications relates to privacy and "does not <u>secure</u> those communications from eavesdropping."

101. The IPsec passage of *H.235* also fails to support the rejection. (*See* Req. at 215-16.) This passage refers to a "call signalling channel," not to an endpoint (*i.e.*, the purported "first device.").

102. It is also my opinion that *H.235* does not explain a relationship or interaction between IPsec and an access token or an access-token-protected alias addresses (*i.e.*, purported "secure" names), much less how IPsec negotiations would proceed between one or more devices employing such tokens. (*H.235* 30-31.) At the same time, *H.235* does not explain whether or how the H.245 channels utilized by IPsec may implement its features through a gatekeeper-routed connection, which is required when access tokens are employed. (*H.323* 38; *H.235* 30, disclosing no gatekeeper functions when a call is established, and disclosing no gatekeeper role at all beyond step 1.)

103. Further, it is my opinion that the "Call establishment security" feature of *H.235* additionally fails to support the rejection. (*See* Req. at 216.) The "connection messages" disclosed in this *H.235* passage occur only *after* security features have already been employed, and therefore these messages cannot correspond to a "message . . . of the desired to securely communicate," as recited in claim 1. (*H.235* 6, "a secure mode of communication should be used . . . *before* the exchange of call connection messages," emphasis added.) Moreover, *H.323* does not describe the "call establishment channel" as a channel between the endpoints, the purported "first device" and "second device" of claim 1. (*See generally H.235*, *H.323* 4-8.) In my opinion, *H.235* also discusses no relationship or interaction between call establishment security and an access token or access-token-protected alias address (*i.e.*, purported "secure" name), let alone how call establishment security would proceed with one or more devices employing such tokens.

104. Additionally, it is my opinion that the "Call control (H.245) security" and "Media stream privacy" passages of *H.235* also fail to support the rejection. (*See* Req. at 216-17.) These passages do not describe receiving any message at a network address corresponding to an access token or an access-token-protected alias address (*i.e.*, the purported secure name). (*H.235* 6-7.) *H.235* also does not explain whether or how the necessary H.245 channels may implement security features through a gatekeeper-routed connection, which is required when access tokens are employed. (*H.235* 6-7; *H.323* 38.) Rather, *H.235* teaches that implementation of the security features in these passages lies within the discretion of the calling endpoint. (*Id.* at 6-7, "The H.245 channel shall be secured using any negotiated privacy mechanism (*this includes the option of 'none'*)," "any participating endpoints *may* utilize an encrypted H.245 channel," emphases added.)

105. One of ordinary skill in the art would have understood that data security (*i.e.*, encryption) must be present to have "secure communication link." Otherwise, a communication link cannot "<u>secure</u> those communications from eavesdropping." Here, the access token section of *H.323* does not involve encrypted communications between endpoints. (*H.323* 38.) The security token

passages of *H.235* only disclose encryption of the tokens themselves, not of any communication link. (*H.235* 28-29.) The "Call establishment security" passage of *H.235* also does not disclose a secure communication link. (*Id.* at 6.) Additionally, in my opinion, *H.235* additionally fails to explain whether or how to implement the IPsec "Call control (H.245) security" and "Media stream privacy" features utilizing H.245 channels in conjunction with access-token-protected aliases, or through gatekeeper-routed connections, which are required when access tokens are employed. (*H.235* 6-7, 30-31; *H.323* 38.)

B. Claim 2

106. I understand the Office and Requester allege that an alias address of a called endpoint protected by an access token corresponds to the secure name recited in independent claim 2. (Req. at 220.) This is incorrect for the reasons I provided above with respect to independent claim 1.

107. In my opinion, the address mentioned in the IPsec passage of *H.235* does not disclose the "network address" of claim 2. Rather, this address corresponds to "the call signalling channel" rather than to the called endpoint (*i.e.*, the purported "second device"). (*H.235* 30-31; *see also H.323* 5, defining these components.)

108. I understand the Office and Requester assert that an alias address protected by an access token corresponds to a "secure name." (OA at 11; Req. at 220.) As I explained above, I disagree with this position. But even if one incorrectly assumes this to be true, using access tokens in *H.323* necessarily prevents the calling endpoint (*i.e.*, the purported "first device") from ever receiving a network address. (*H.323* 38.) *H.323* specifies that access tokens "provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party." (*H.323* 38.) An access token requires routing communications through a gatekeeper because the "[g]atekeeper will know the endpoint related to the Access Token," unlike the calling endpoint. (*Id.*) Indeed, *H.323* states "A user may give out *only* the Access Token for a calling party to use in reaching the endpoint." (*Id.*) Thus, a calling endpoint using an access token never receives a network address associated with the access-token-protected alias address.

109. I further understand that the Requester relies on the security token passage of *H.235* as disclosing the "sending a message to a secure name service" and "receiving a message containing the network address" features of claim 2. (Req. at 218-23.) In my opinion, however, the *H.235* security token feature does not utilize an alias address protected by an access token. (*H.235* 28-29.)

110. I understand the Requester further relies on the IPsec passage of *H.235* to support the rejection, asserting that "H.323 secures the name of an Alias address via IPsec when the calling

endpoint queries the Gatekeeper." (Req. at 221-22.) I disagree. The IPsec passage explains that "the gatekeeper will inform the endpoint of the address and port number of the call signalling channel" over a pre-existing secure RAS channel. (*H.235* 30, step 1.) Thus, *H.235* explains that the *RAS* channel is secure—not that any name allegedly provided to the gatekeeper is secure. (*H.235* 30, step 1.) Furthermore, the address provided by the gatekeeper corresponds to a "call signalling channel," not to a called endpoint (the purported "second device").

111. I understand that independent claim 2 also recites, "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." For similar reasons as I discussed above with respect to claim 1, the "Call establishment security," "Call control (H.245) security, and "Media stream privacy" features of *H.235* all fail to disclose a "secure communication link."

112. I understand the Requester additionally relies on the IPsec passage of *H.235* in its analysis of claim 2. Although *H.235* discloses a gatekeeper participating in returning an address and port number to the calling endpoint, (*H.235* at 30, step 1), it does not disclose whether or how encryption would be employed over a gatekeeper-routed H.245 channel, which is required when access-token-protected alias addresses (*i.e.*, the purported "secure" names) are employed. (*Id.* at 30-31; *H.323* 38.) Instead, *H.235* explains that person-to-person Q&A authentication measures may occur, which is inconsistent with a gatekeeper-routed connection. (*H.235* 30.) *H.235* also explains that routing H.245 channels through various intermediate devices, including *proxies* and firewalls, is incompatible with employing encryption on those channels. (*H.235* 31.) And finally, the only address disclosed with respect to the IPsec passage corresponds to a "call signalling channel," not the alleged "second device" (*i.e.*, a called endpoint) of claim 2. (*H.235* 30.)

C. Claim 4

113. Having identified an alias address protected by an access token as the "secure name" recited in claims 1 and 2, (*see* Req. at 209, 220), or a name in the IPsec passage of *H.235* of a "call signalling channel," (*id.* at 221), I understand the Requester now contends that a third feature discloses a "secure name" that "indicates security": the *H.235* security token passage. (*Id.* at 227.) But as I discussed above with respect to claim 2, the access token and security token features are distinct, and the IPsec passage does not discuss using either access tokens or security tokens.

114. Furthermore, I understand the Requester bases its "secure name" arguments regarding the *H.323* access token section and the *H.235* IPsec passages on features that merely shield names from other entities and do not indicate any security.

D. Claim 5

115. For the additional claim 5 feature of "receiving the message in encrypted form," I understand the Requester relies exclusively on the IPsec passage of *H.235*. But because the address returned in the IPsec passage corresponds to a "call signalling channel," rather than the endpoint earlier identified as the "second device," this passage fails to support the rejection.

E. Claims 10 and 11

116. I understand the Office asserts that the tunneling features of claims 10 and 11 are disclosed by the "Encapsulation" passage of *H.323*. (OA at 11-12, quoting *H.323* 59.) But it is my opinion that this passage does not disclose receiving any message containing a network address "through tunneling," as recited in claim 10, or "in the form of at least one tunneled packet," as recited in claim 11. The tunneling discussed on page 59 involves H.245 channels and messages, while the gatekeeper (purported "secure name service") communicates with endpoints through H.225 signalling. (*H.323* 27.) The *H.235* IPsec passage cited in the Request only discloses an address corresponding to a "call signalling channel"—not an endpoint (*i.e.*, alleged "second device")—as discussed above. (*See* OA at 11-12; Req. at 231.)

F. Claim 13

117. *H.323* explains that its layering feature should employ a separate channel and a separate session, unlike the additional feature of claim 13, which recites that one "secure communication link includes multiple sessions." (*H.323* at 91.) Moreover, as I mentioned above with respect to claims 1 and 2, the combined *H.323* references do not disclose any "secure communication link," as recited in claim 13.

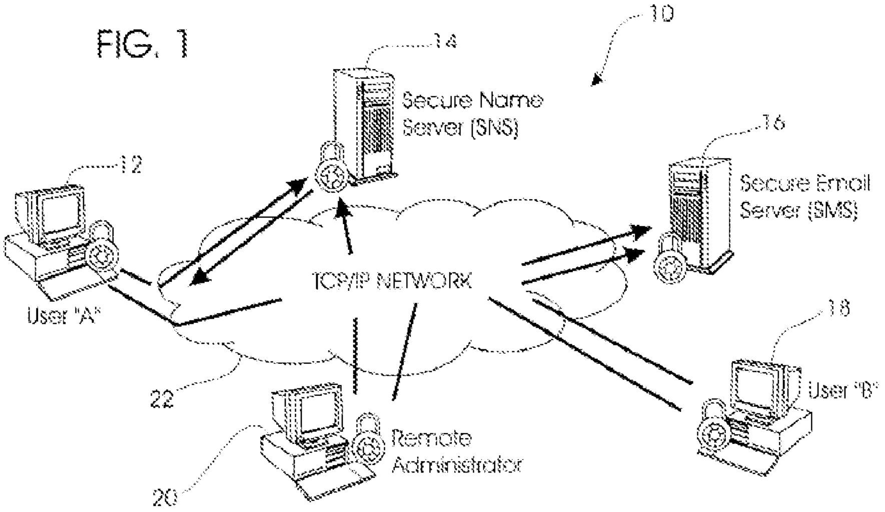
G. Claims 21, 24, 26, 28, and 29

118. I understand that independent claims 21, 24, 26, 28, and 29 recite features similar to one or more features of independent claims 1 and 2, discussed above. My opinions expressed above regarding claims 1 and 2 also apply to claims 21, 24, 26, 28, and 29, to the extent these claims recite similar features.

X. JOHNSON IN VIEW OF RFC 2131, RFC 1034, AND RFC 2401

119. I understand that *Johnson* generally relates to "a secure electronic mail communication system . . . for use in communicating over networks where secure information exchange is required." (*Johnson* 1:20-23.) With reference to Fig. 1, reproduced below, *Johnson* discloses that the secure mail server 16 obtains a dynamic address from the connecting network 22 and notifies the secure name server 14 of the obtained dynamic address. (*Johnson* 6:25-34.)

FIG. 1



When a first user 12 desires to send an email to a second user 18, the first user 12 uses his "logon protocol combination to access the secure name server 14 over the connecting network 22," (*Johnson* 7:13-14), which in one embodiment may include selecting a "fixed address/name" of the secure name server 14. (*Johnson* 11:23-24.) The first user 12 "obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14" (*Johnson* 7:15-17); in one embodiment the "secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message." (*Johnson* 8:4-6.) The first user 12 then uses "his ID/password combination and the dynamic address to log onto the secure electronic mail server 16." (*Johnson* 7:20-22.) "[T]he first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16." (*Johnson* 7:23-27.) A second user may subsequently use his "logon protocol to obtain the dynamic address of the electronic mail server 16 from the secure name server 14 and then access the secure electronic mail server 16 with his ID/Password combination." (*Johnson* 7:31-35.) Thus, "the first user 12 and the second user 18 never communicate directly." (*Johnson* 7:54-55.)

120. *RFC 2131* generally relates to a Dynamic Host Configuration Protocol (DHCP) that "provides a framework for passing configuration information to hosts on a TCPIP network." (*RFC 2131* at 1.) *RFC 1034* generally relates to "an introduction to the Domain Name System (DNS)." (*RFC 1034* at 1.) *RFC 2401* generally relates to a Security Architecture for the Internet Protocol that "addresses security only at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms." (*RFC 2401* at 3.)

A. Independent Claim 1

121. I understand that claim 1 recites "a first device associated with a secure name and an unsecured name." In my opinion, *Johnson* does not disclose any "secure names." As I explained above regarding *Provino*, "secure names" are those names used to communicate securely that are resolved by a secure name service (*i.e.*, a service that both resolves a name into a network address and further supports establishing a secure communication link). In my opinion, the server 14 in *Johnson* is a conventional name server of the type distinguished in the '181 patent specification and does not qualify as a "secure name service" that can resolve "secure names." Instead, when provided with the name of secure mail server 16, the secure name server 14 merely returns the dynamic address of the secure mail server 16. (*Johnson* 7:15-17, 8:4-6.) Server 14 does not provide any further support for establishing a secure communication link.

122. I understand that the Office and Requester contend that the secure mail server 16 of *Johnson* corresponds to the claimed "first device," and that a name purportedly registered "by the secure mail server with the secure name server is a 'secure name' . . . because it requires, for example, authorization to access and is protected through encryption." (Req. at 272.) I disagree with the Office and the Requester, even granting the Office and the Requester their definition of "secure name." *Johnson* discloses that the *dynamic address* of the secure mail server 16 (as opposed to a *name* of the secure mail server 16) is purportedly "not easily obtained" because the secure name server 14 "requires a proper log protocol combination to access" and because "secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message." (*Johnson* 8:1-8.) *Johnson* does not teach or suggest that the *name* of secure mail server 16 is protected through authorization and encryption. Indeed, the user accessing the secure name server 14 must presumably already know the name of the secure mail server 16 before the purported authorization and encryption ever happens, because if the user did not already know the name, it would not know how to request the dynamic address of secure mail server 16 from secure name server 14. For example, as shown in *Johnson's* Figure 2, a user must obtain the secure mail server IP address from the secure name server, but to do so, the user must log in to the secure name server and provide the name of the secure mail server. (*See, e.g., Johnson* 9:23-33.) Thus, the user must already know the name of the secure mail server before obtaining its IP address. In my opinion, there is no disclosure in *Johnson* regarding how the user initially learns this name, whether authorization is required before obtaining the name, or whether encryption is used in providing the name. Accordingly, Requester and the Office have not demonstrated that *Johnson* discloses or

suggests a "secure name" even under their own interpretation of that term.

123. Further, in my opinion, the Office and Requester are incorrect that the claimed "unsecured name" is met by a domain name of the secure name server 14, purportedly registered with a DHCP server or in a public DNS system. (Req. at 273-274.)

124. Both positions (regarding registration of secure name server 14 with a DHCP server or in the public DNS system) rely on the premise that the secure name server 14 must have a registered domain name, which the Office and Requester contend is "necessary to the invention of Johnson" for *Johnson* to be used in "communications over the Internet." (Req. at 274.) I disagree, because a registered domain name is not a prerequisite for communications over the Internet. In fact, communications over the Internet existed well before the creation of *RFC 1034* that is asserted by the Office and Requester as disclosing domain name registration.

125. Finally, the Office and Requester allege that "the secure mail server has a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an 'unsecured name'." (Req. at 274.) I disagree because the secure mail server 16 is only disclosed to have its name registered in secure name server 14.

126. I understand that claim 1 further recites "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." *Johnson* and the other cited references do not disclose or suggest a "secure name" for the reasons I discuss above.

127. I understand that claim 1 further recites "sending a message over a secure communication link from the first device to the second device." The Office and Requester contend that the email message of the first user 12 (purported "second device") that is transmitted to the secure mail server 16 (purported "first device") discloses or suggests this feature. (Req. at 274-275.) They have it reversed. The email message of the first user 12 (purported "second device") is sent to a mailbox on the secure mail server 16 (purported "first device"), not from the purported "first device" to the purported "second device." (*Johnson* 7:23-27.)

128. The Office and Requester additionally contend that the email of the first user 12 is both "a message from a second device of the desire[] to securely communicate," and "a message . . . from the first device to the second device." (Req. at 275.) But, in my opinion, one of ordinary skill in the art would recognize that the email from the first user 12 cannot be both "a message from a second device" and "a message . . . to the second device."

B. Dependent Claim 3

129. I understand dependent claim 3 depends from independent claim 2 and further recites, among other things, that "the secure name of the second device is a secure domain name." As I previously discussed with respect to claim 1, I disagree that *Johnson* teaches that the secure mail server 16 (purported "second device") has a "secure name," a feature which claims 2 and 3 also contain.

130. Still, in their analysis of claim 3, the Office and Requester contend that the Domain Name System ("DNS") teachings of *RFC 1034*, combined with *Johnson*, disclose or suggest that the name of the secure mail server 16 can be a secure domain name. (Req. at 283-284.) In support of this position, the Office and Requester combine *RFC 1034*'s teaching of an authoritative name server with the secure name server 14 of *Johnson* to conclude that the secure name server 14 is "the authoritative name server for the protected network." (Req. at 283-284.) But there is no indication of how *Johnson* would determine which of its multiple name servers, if any, would function as the authoritative name server. (*See id.* at 282-84.)

C. Dependent Claim 7

131. I understand that dependent claim 7 recites, among other things, that "the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." I understand that the Office and Requester contend that a secure communication link would not be utilized during registration of a secure mail server 16 in *Johnson's* embodiment where the secure name server 14 and the secure mail server 16 reside on the same computer system, but that a secure communication link is purportedly utilized during the registration of the secure mail server 16 in *Johnson's* other embodiments. (Req. at 287.) I disagree, because there is no disclosure or suggestion in *Johnson* that the registration process changes if the secure name server 14 and the secure mail server 16 reside on the same computer system. Instead, *Johnson* discloses that in this embodiment, "two separate communication lines would be necessary to allow for the fixed address of the secure name server while providing for a dynamic address of the secure mail server." (*Johnson* 12:20-25.) Accordingly, one of ordinary skill in the art would recognize that the servers 14 and 16 still communicate over the network via the two separate communication lines, thus warranting no change in their operation and certainly no change that would result in communications having weakened or no security.

D. Claims 21-29

132. I understand that claims 21-29 include features similar to those I have discussed above with respect to other claims of the '181 patent. Accordingly, my opinions expressed above regarding these claims 21-29.

Truth and Accuracy of Statements

1. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that willful false statements or the like may jeopardize the validity of the '181 patent.

Signed at New York, New York, this 4th day of September, 2012.

/Angelos D. Keromytis/

Angelos D. Keromytis

Angelos D. Keromytis - *Curriculum Vitae*

Positions Held

- **January 2006 - Present**
  Associate Professor, Department of Computer Science, Columbia University, New York.
- **January 2009 - January 2010**
  Senior Research Engineer, Symantec Research Labs Europe, Sophia Antipolis, France.
- **July 2001 - December 2005**
  Assistant Professor, Department of Computer Science, Columbia University, New York.
- **September 1996 - July 2001**
  Research Assistant, Computer and Information Science Department, University of Pennsylvania, Philadelphia.
- **January 1993 - October 1995**
  Member of the Technical Staff, FORTHnet S.A., Heraclion, Greece.
- **September 1991 - January 1993**
  Member of the Technical Staff, Education Team, Computer Center of the University of Crete, Heraclion, Greece.

Education

- **November 2001**
  Ph.D. (Computer Science), University of Pennsylvania, USA.
- **August 1997**
  M.Sc. (Computer Science), University of Pennsylvania, USA.
- **June 1996**
  B.Sc. (Computer Science), University of Crete, Greece.

Service and Teaching

Editorial Boards and Steering Committees

- Associate Editor, Encyclopedia of Cryptography and Security (2nd Edition), Springer, 2010 - 2011.
- Associate Editor, IET (formerly IEE) Proceedings Information Security, 2005 - 2010.
- Steering Committee, *ISOC Symposium on Network and Distributed System Security (SNDSS),* 2006 - 2009.
- Steering Committee, *New Security Paradigms Workshop (NSPW),* 2007 onward.
- Associate Editor, ACM Transactions on Information and System Security (TISSEC), 2004 - 2010.
- Steering Committee, *USENIX Workshop on Hot Topics in Security (HotSec),* 2006 - 2009.
- Steering Committee, *Computer Security Architecture Workshop (CSAW),* 2007 - 2009.

Program Chair

- Program Chair, 16th International Conference on Financial Cryptography and Data Security (FC), 2012.
- Program co-Chair, 17th ACM Computer and Communication Security (CCS), 2010.
- Program co-Chair, 16th ACM Computer and Communication Security (CCS), 2009.
- Program co-Chair, New Security Paradigms Workshop (NSPW), 2008.
- Program co-Chair, New Security Paradigms Workshop (NSPW), 2007.
- Chair, 27th International Conference on Distributed Computing Systems (ICDCS), *Security*

Track, 2007.

- Chair, 16th World Wide Web (WWW) Conference, *Security, Privacy, Reliability and Ethics Track,* 2007.
- Chair, 15th USENIX Security Symposium, 2006.
- Deputy Chair, 15th World Wide Web (WWW) Conference, *Security, Privacy and Ethics Track,* 2006.
- Chair, 3rd Workshop on Rapid Malcode (WORM), 2005.
- Program co-Chair, 3rd Applied Cryptography and Network Security (ACNS) Conference, 2005.
- Program co-Chair, OpenSig Workshop, 2003.

Program Organization

- General Chair, New Security Paradigms Workshop (NSPW), 2010.
- General Vice Chair, New Security Paradigms Workshop (NSPW), 2009.
- Co-chair, Invited Talks, 17th USENIX Security Symposium, 2008.
- General co-chair, Applied Cryptography and Network Security (ACNS) Conference, 2008.
- Co-chair, Invited Talks, 16th USENIX Security Symposium, 2007.
- Organizing Committee, Columbia/IBM/Stevens Security & Privacy Day (bi-annual event).
  - Organizer, Columbia/IBM/Stevens Security & Privacy Day, December 2010.
  - Organizer, Columbia/IBM/Stevens Security & Privacy Day, June 2007.
- Co-organizer, ARO/FSTC Workshop on Insider Attack and Cyber Security, 2007.
- Publicity co-Chair, ACM Conference on Computer and Communications Security, 2006.
- General co-Chair, OpenSig Workshop, 2003.

Program Committees

- Program Committee, ISOC Symposium on Network and Distributed Systems Security (SNDSS), 2003, 2004, 2006, 2007, 2008, 2012.
- Program Committee, International Workshop on Security (IWSEC), 2006, 2007, 2008, 2009, 2010, 2011.
- Program Committee, ACM Conference on Computer and Communications Security (CCS), 2005, 2007, 2008, 2009, 2010.
- Program Committee, Applied Cryptography and Network Security (ACNS) Conference, 2005, 2006, 2010, 2011, 2012.
- Program Committee, USENIX Security Symposium, 2004, 2005, 2006, 2008.
- Program Committee, International Conference on Distributed Computing Systems (ICDCS), *Security Track*, 2005, 2006, 2007, 2008.
- Program Committee, Workshop on Rapid Malcode (WORM), 2004, 2005, 2006, 2007.
- Program Committee, Information Security Conference (ISC), 2005, 2007, 2009, 2011.
- Program Committee, World Wide Web Conference (WWW), 2005, 2006, 2007.
- Program Committee, USENIX Workshop on Hot Topics in Security (HotSec), 2006, 2007, 2010.
- Program Committee, Financial Cryptography (FC) Conference, 2002, 2010, 2011, 2012.
- Program Committee, European Workshop on Systems Security (EuroSec), 2009, 2010, 2011.
- Program Committee, Annual Computer Security Applications Conference (ACSAC), 2006, 2007, 2011.
- Program Committee, USENIX Technical Conference, *Freely Distributable Software (Freenix) Track,* 1998, 1999, 2003.
- Program Committee, IEEE Security & Privacy Symposium, 2006, 2008.
- Program Committee, ACM SIGCOMM Workshop on Large Scale Attack Defense (LSAD), 2006, 2007.

- Program Committee, New Security Paradigms Workshop (NSPW), 2007, 2008.
- Program Committee, IEEE WETICE Workshop on Enterprise Security, 2002, 2003.
- Program Committee, International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS), 2007, 2010.
- Program Committee, USENIX Annual Technical Conference (ATC), 2008, 2011.
- Program Committee, European Sumposium on Research in Computer Security (ESORICS), 2011.
- Program Committee, International Workshop on Mobile Security (WMS), 2010.
- Program Committee, 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Dependable Computing and Communication Symposium (DCCS), 2010.
- Program Committee, Computer Forensics in Software Engineering Workshop, 2009.
- Program Committee, USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET), 2008.
- Program Committee, 23rd International Information Security Conference (IFIP SEC), 2008.
- Program Committee, Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM), 2008.
- Program Committee, 1st Computer Security Architecture Workshop (CSAW), 2007.
- Program Committee, 8th IEEE Information Assurance Workshop (IAW), 2007.
- Program Committee, Anti-Phishing Working Group (APWG) eCrime Researchers Summit, 2007.
- Program Committee, 4th GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA), 2007.
- Program Committee, 2nd ACM Symposium on InformAtion, Computer and Communications Security (AsiaCCS), 2007.
- Program Committee, 6th International Conference on Cryptology and Network Security (CANS), 2007.
- Program Committee, 2nd Workshop on Advances in Trusted Computing (WATC), 2006.
- Program Committee, International Conference on Information and Communications Security (ICICS), 2006.
- Program Committee, 2nd Workshop on Secure Network Protocols (NPSec), 2006.
- Program Committee, 1st Workshop on Hot Topics in System Dependability (HotDep), 2005.
- Program Committee, 20th ACM Symposium on Applied Computing (SAC), Trust, Recommendations, Evidence and other Collaboration Know-how (TRECK) Track, 2005.
- Program Committee, 1st Workshop on Operating System and Architecture Support for the on demand IT Infrastructure (OASIS), 2004.
- Program Committee, Workshop on Information Security Applications (WISA), 2004.
- Program Committee, Workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI), 2004.
- Program Committee, 29th IEEE Conference on Local Computer Networks (LCN), 2004.
- Program Committee, 2nd International Conference on Trust Management, 2004.
- Program Committee, Asia BSD Conference, 2004.
- Program Committee, 2nd Annual New York Metro Area Networking Workshop (NYMAN), 2002.
- Program Committee, Cloud Computing Security Workshop (CCSW), 2009.
- Program Committee, Workshop on Grid and Cloud Security (WGC-Sec), 2011.
- Program Committee, Workshop on Cyber Security Experimentation and Test (CSET), 2011.

Advisory Workshops

- ODNI/NSA Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E), Keystone, CO, September 2011.
- ONR Workshop on Host Computer Security, Chicago, IL, October 2010.
- Intel Workshop on Trust Evidence and End-to-end Trust in Heterogeneous Environments, Santa Clara, CA, May 2010.
- Intelligence Community Technical Exchange on Moving Target, Washington, DC, April 2010.
- Lockheed Martin Future Security Threats Workshop, New York, NY, November 2009.
- Air Force Office for Scientific Research (AFOSR) Invitational Workshop on Homogeneous Enclave Software *vs* Heterogeneous Enclave Software, Arlington, VA, October 2007.
- NSF Future Internet Network Design Working Meeting, Arlington, VA, June 2007.
- ARO/FSTC Workshop on Insider Attack and Cyber Security, Arlington, VA, June 2007.
- NSF Invitational Workshop on Future Directions for the CyberTrust Program, Pittsburgh, PA, October 2006.
- ARO/HSARPA Invitational Workshop on Malware Detection, Arlington, VA, August 2005.
- Department of Defense Invitational Workshop on the Complex Behavior of Adaptive, Network-Centric Systems, College Park, MD, July 2005.
- ARDA Next Generation Malware Invitational Workshop, Annapolis Junction, MD, March 2005.
- Co-leader of session on "Securing software environments", joint NSF and Department of Treasury Invitational Workshop on Resilient Financial Information Systems, Washington, DC, March 2005.
- DARPA Application Communities Invitational Workshop, Arlington, VA, October 2004.
- DARPA APNets Invitational Workshop, Philadelphia, PA, December 2003.
- NSF/NIST Invitational Workshop on Cybersecurity Workforce Needs Assessment and Educational Innovation, Arlington, VA, August 2003.
- NSF Invitational Workshop on Large Scale Cyber-Security, Lansdowne, VA, March 2003.
- IP Security Working Group Secretary, Internet Engineering Task Force (IETF), 2003 - 2008.
- Session moderator, Workshop on Intelligence and Research, Florham Park, NJ, October 2001.
- DARPA Composable High Assurance Trusted Systems #2 (CHATS2) Invitational Workshop, Napa, CA, November 2000.

Other Professional Activities

- Co-chair, ACM Computing Classification System Update Committee ("Security and Privacy" top-level node), 2011.
- Member, ACM Computing Classification System Update Committee (top two levels), 2010.
- External Advisory Board member, *"i-code: Real-time Malicious Code Identification"*, EU project, 2010 - 2012.
- Reviewer (grant applications), Greek Ministry of Education, 2010.
- Reviewer (grant applications), Danish National Research Foundation, 2010.
- Member of the Scientific Advisory Board, Centre for Research and Technology, Hellas (CERTH), 2008 - 2011.
- Senior Member of the ACM, 2008 onward.
- Senior Member of the IEEE, 2009 onward.
- Visiting Scientist, Institute for Infocomm Research (I^2R), Singapore, February - May 2007.
- Columbia Representative to the Institute for Information Infrastructure Protection (I3P), 2006 - 2008.
- Technical Advisory Board, *StackSafe Inc. (formerly Revive Systems Inc.),* 2006 - 2009.

- Technical Advisory Board, *Radiuz Inc.,* 2006.
- Reviewer (grant applications), Institute for Security Technology Studies (ISTS), Dartmouth College, 2006.
- Reviewer, Singapore National Science and Technology Awards (NSTA), 2006.
- Board of Directors, *StackSafe Inc.(formerly Revive Systems Inc.),* 2005 - 2009.
- Founder, *StackSafe Inc. (formerly Revive Systems Inc.),* 2005 - 2009.
- Expert witness in criminal and intellectual property litigation cases, 2005, 2006, 2007, 2009, 2010, 2011.
- Science Fair Judge, Middle School for Democracy and Leadership, Brooklyn, NY, 2005, 2006.
- Reviewer (grant applications), Swiss National Science Foundation, 2007.
- Reviewer (grant applications), Netherlands Organisation for Scientific Research, 2005, 2006.
- Reviewer (grant applications), US/Israel Binational Science Foundation, 2003, 2005.
- NSF reviewer & panelist, 2002, 2003, 2006, 2008, 2009, 2011.
- Internet Engineering Task Force (IETF) Security Area Advisor, 2001 - 2008.

Ph.D. Thesis Committee Service

- Michalis Polychronakis, *"Generic Code Injection Attack Detection using Code Emulation",* Computer Science Department, University of Crete, October 2009.
- Spyros Antonatos, *"Defending against Known and Unknown Attacks using a Network of Affined Honeypots",* Computer Science Department, University of Crete, October 2009.
- Van-Hau Pham, *"Honeypot Traces Forensics by Means of Attack Event Identification",* Computer Science Group, Communications and Electronics Department, Ecole Nationale Superieure des Telecommunications, September 2009.
- Gabriela F. Ciocarlie, *"Towards Self-Adaptive Anomaly Detection Sensors",* Department of Computer Science, Columbia University, September 2009.
- Vanessa Frias-Martinez, *"Behavior-Based Admission and Access Control for Network Security",* Department of Computer Science, Columbia University, September 2008.
- Wei-Jen Li, *"SPARSE: A Hybrid System for Malcode-Bearing Document Detection",* Department of Computer Science, Columbia University, June 2008.
- Raj Kumar Rajendran, *"The Method for Strong Detection for Distributed Routing",* Electrical Engineering Department, Columbia University, March 2008.
- Constantin Serban, *"Advances in Decentralized and Stateful Access Control",* Computer Science Department, Rutgers University, December 2007.
- Ricardo A. Baratto, *"THINC: A Virtual and Remote Display Architecture for Desktop Computing",* Computer Science Department, Columbia University, October 2007.
- Zhenkai Liang, *"Techniques in Automated Cyber-Attack Response and Recovery",* Computer Science Department, Stony Brook University, November 2006.
- Ke Wang, *"Network Payload-based Anomaly Detection and Content-based Alert Correlation",* Computer Science Department, Columbia University, August 2006.
- Seoung-Bum Lee, *"Adaptive Quality of Service for Wireless Ad hoc Networks",* Electrical Engineering Department, Columbia University, June 2006.
- Shlomo Hershkop, *"Behavior-based Email Analysis with Application to Spam Detection",* Computer Science Department, Columbia University, August 2005.
- Gaurav S. Kc, *"Defending Software Against Process-subversion Attacks",* Computer Science Department, Columbia University, April 2005.
- Gong Su, *"MOVE: A New Virtualization Approach to Mobile Communication",* Computer Science Department, Columbia University, May 2004.
- Jonathan M. Lennox, *"Services for Internet Telephony",* Computer Science Department,

Columbia University, December 2003.

- Michael E. Kounavis, *"Programming Network Architectures"*, Electrical Engineering Department, Columbia University, June 2003.
- Wenyu Jiang, *"QoS Measurement and Management for Internet Real-time Multimedia Services"*, Computer Science Department, Columbia University, April 2003.

Post-doctoral Students

- Hyung Chan Kim (October 2007 - October 2008)
- Stelios Sidiroglou (October 2008 - December 2008)
- Georgios Portokalidis (March 2010 - present)
- Michalis Polychronakis (May 2010 - present)
- Dimitris Geneiatakis (June 2010 - present)

Current Ph.D. Students

- Georgios Kontaxis (September 2011)
- Vasilis Pappas (September 2009 - present)
- Vasileios Kemerlis (September 2008 - present)
- Kangkook Jee (January 2008 - present)
- Sambuddho Chakravarty (January 2007 - present)
- Angelika Zavou (September 2006 - present)

Graduated Ph.D. Students

- Debra Cook (January 2002 - June 2006)
  - Thesis title: *"Elastic Block Ciphers"*
  - Post-graduation: Member of the Technical Staff, Bell Labs
  - Currently: Research Staff Member, Telcordia Research
- Angelos Stavrou (January 2003 - August 2007)
  - Thesis title: *"An Overlay Architecture for End-to-End Service Availability"* (awarded with distinction)
  - Post-graduation: Assistant Professor, Computer Science Department, George Mason University (GMU)
  - Currently: Assistant Professor, Computer Science Department, George Mason University (GMU)
- Michael E. Locasto (September 2002 - December 2007)
  - Thesis title: *"Integrity Postures for Software Self-Defense"* (awarded with distinction)
  - Post-graduation: ISTS Research Fellow, Dartmouth College
  - Currently: Assistant Professor, Department of Computer Science, University of Calgary
- Stelios Sidiroglou (June 2003 - May 2008)
  - Thesis title: *"Software Self-healing Using Error Virtualization"*
  - Post-graduation: Research Scientist, Columbia University
  - Currently: Research Scientist, MIT CSAIL
- Mansoor Alicherry (September 2006 - October 2010)
  - Thesis title: *"A Distributed Policy Enforcement Architecture for Mobile Ad Hoc Networks"*
  - Post-graduation: Member of the Technical Staff, Alcatel-Lucent Bell Labs
  - Currently: Member of the Technical Staff, Alcatel-Lucent Bell Labs
- Brian Bowen (September 2007 - December 2010; co-advised with Salvatore J. Stolfo)
  - Thesis title: *"Design and Analysis of Decoy Systems for Computer Security"*
  - Post-graduation: Member of the Technical Staff, Sandia National Laboratories

    - Currently: Member of the Technical Staff, Sandia National Laboratories

Service at Columbia

- Computer Science Department Ph.D. Committee, 2010 - 2011
- Computer Science Department Facilities committee, 2001 - 2008, 2010 - current
    - Chair, Facilities committee, 2003 - 2005, 2011 - current
- M.Sc. Admissions committee, 2007 - current.
- M.Sc. Committee, 2008 - current.
- Computer Science Department Faculty Recruiting committee, 2002, 2008
- Columbia committee on Research Conflict of Interest Policy, 2007 - 2008
- Co-organizer, Computer Science Faculty Retreat, Fall 2007
- Advisor for the School of Engineering Computer Science Majors, Freshmen & Sophomores, 2004 - 2005
- Computer Science Department Undergraduate Admissions Representative, 2003 - 2008
- Advisor for the School of Engineering Computer Science Majors, Seniors, 2003 - 2004, 2006 - 2007
- Computer Science Department Space Allocation Policy committee, 2002 - 2010
- Computer Science Department Events Representative, 2002 - 2008
- Advisor for the School of Engineering Computer Science Majors, Juniors, 2002 - 2003, 2005 - 2006
- Computer Science Department CRF Director Hiring committee, 2003
- Advisor for the School of Engineering Computer Science Majors, Sophomores, 2001 - 2002
- Computer Science Department Faculty Recruiting committee, 2001 - 2002
- Executive Vice Provost committee on Columbia's response to the 9/11 events, Fall 2001

Teaching

(Scores indicate mean course quality rating from student survey; survey not conducted for summer sessions)

- Instructor, COMS E6183-1 - Advanced Topics in Network Security, Columbia University
    - Fall 2006: 17 on-campus students *(4.58/5)*
- Instructor, COMS W6998.1 - Advanced Topics in Network Security, Columbia University
    - Fall 2004: 17 on-campus students *(4.62/5)*
    - Spring 2003: 18 on-campus students *(N/A)*
- Instructor, COMS W4180 - Network Security, Columbia University
    - Spring 2011: 4 CVN students *(N/A)*
    - Fall 2010: 2 CVN students *(N/A)*
    - Spring 2010: 25 on-campus and 5 CVN students *(4.48/5)*
    - Summer 2006: 7 CVN students *(N/A)*
    - Spring 2006: 63 on-campus and 9 CVN students *(4.14/5)*
    - Summer 2005: 4 CVN students *(N/A)*
    - Spring 2005: 41 on-campus and 5 CVN students *(4.25/5)*
    - Summer 2004: 6 CVN students *(N/A)*
    - Fall 2003: 45 on-campus and 12 CVN students *(3.74/5)*
    - Summer 2003: 5 CVN students *(N/A)*
    - Fall 2002: 43 on-campus and 9 CVN students *(3.21/5)*
    - Fall 2001: 23 on-campus students *(3.6/5)*
- Instructor, COMS W4118 - Operating Systems, Columbia University
    - Summer 2007: 8 CVN students *(N/A)*
    - Fall 2006: 59 on-campus and 7 CVN students *(3.73/5)*

  - Summer 2006: 15 CVN students *(N/A)*
  - Fall 2005: 52 on-campus and 9 CVN students *(3.86/5)*
  - Spring 2004: 32 on-campus and 4 CVN students *(3.39/5)*
  - Spring 2002: 37 on-campus students *(3.13/5)*
- Instructor, COMS W3157 - Advanced Programming, Columbia University
  - Fall 2010: 37 on-campus students *(3.25/5)*
  - Fall 2007: 30 on-campus students *(4.16/5)*
- Instructor, CIS700/002 - Building Secure Systems, University of Pennsylvania, Spring 1998

Support for Research and Teaching (Gifts and Grants)

1. PI (co-PIs: Roxana Geambasu, Junfeng Yang, Simha Sethumadhavan, Sal Stolfo), *"MEERKATS: Maintaining EnterprisE Resiliency via Kaleidoscopic Adaptation & Transformation of Software Services"*, DARPA MRC, **$6,619,270** (09/2011 - 09/2015; leading team that includes George Mason University and Symantec Corp.)
2. PI, *"NSF Support for the 2011 New Security Paradigms Workshop Financial Aid (Supplement)"*, NSF Trustworthy Computing, **$10,000** (06/2011 - 07/2012)
3. PI, *"Leveraging the Cloud to Audit Use of Sensitive Infomation"*, Google (research gift), **$60,200** (05/2011)
4. co-PI (with Sal Stolfo), *"ADAMS Advanced Behavioral Sensors (ABS)"*, DARPA ADAMS, **$780,996** (05/2011 - 04/2013)
5. PI, *"Tracking Sensitive Information Flows in Modern Enterprises"*, Intel, **$84,951** (12/2010 - 12/2011)
6. co-PI (with Simha Sethumadhavan, Sal Stolfo, Junfeng Yang, and David August @ Princeton), *"SPARCHS: Symbiotic, Polymorphic, Autotomic, Resilient, Clean-slate, Host Security"*, DARPA CRASH, **$6,424,180** (10/2010 - 09/2014)
7. PI, *"NSF Support for the 2010 New Security Paradigms Workshop Financial Aid"*, NSF Trustworthy Computing, **$10,000** (09/2010 - 08/2011)
8. PI (co-PIs: Junfeng Yang, Sal Stolfo), *"MINESTRONE"*, IARPA, **$7,530,113** (08/2010 - 07/2014; leading team that includes Stanford University, George Mason University, and Symantec Corp.)
9. co-PI (with Junfeng Yang and Dawson Engler @ Stanford), *"Seed: CSR: Large: Collaborative Research: SemGrep: Improving Software Reliability Through Semantic Similarity Bug Search"*, NSF CSR, CNS-10-12107, **$325,000** (07/2010 - 06/2011)
10. PI, *"Tracking Sensitive Information Flows in Modern Enterprises"*, Intel, **$82,286** (08/2009 - 07/2010)
11. PI, *"Supplement for International Research Collaborations"*, NSF Trustworthy Computing, $41,769 (09/2009 - 08/2011)
12. PI, *"NSF Support for the 2009 New Security Paradigms Workshop Financial Aid"*, NSF Trustworthy Computing, **$10,000** (09/2009 - 08/2010)
13. PI, *"Measuring the Health of Internet Routing: A Longitudinal Study"*, Google (research gift), **$60,000** (07/2009)
14. PI, *"CSR: Small: An Information Accountability Architecture for Distributed Enterprise Systems"*, NSF Trustworthy Computing, CNS-09-14312, **$450,000** (07/2009 - 06/2012)
15. co-PI (with Jason Nieh), *"TC: Small: Exploiting Software Elasticity for Automatic Software Self-Healing"*, NSF Trustworthy Computing, CNS-09-14845, **$450,000** (07/2009 - 06/2012)
16. co-PI (with Steve Bellovin and Sal Stolfo), *"Pro-actively Removing the Botnet Threat"*, Office of Naval Research (ONR), **$294,625** (04/2009 - 09/2010)
17. co-PI (with Simha Sethumadhavan and Sal Stolfo), *"SCOPS: Secure Cyber Operations and Parallelization Studies Cluster"*, Air Force Office for Scientific Research (AFOSR),

$650,000 (04/15/2009 - 04/14/2010)

18. PI (co-PIs: Sal Stolfo), *"Program Whitelisting, Vulnerability Analytics and Risk Assessment"*, Symantec (research gift), **$65,000** (12/2008)
19. co-PI (with Sal Stolfo), *"Automated Creation of Network and Content Traffic For the National Cyber Range"*, DARPA/STO, **$85,000** (01/01/2009 - 06/30/2011; part of a larger project)
20. co-PI (with Steve Bellovin, Tal Malkin, and Sal Stolfo), *"Secure Encrypted Search"*, IARPA, $648,787 (09/2008 - 02/2010)
21. PI, *"Tracking Sensitive Information Flows in Modern Enterprises"*, Intel (research gift), $64,000 (05/2008)
22. PI, *"Privacy and Search: Having it Both Ways in Web Services"*, Google (research gift), $50,000 (03/2008)
23. PI (co-PI: Sal Stolfo), *"Continuation: Safe Browsing Through Web-based Application Communities"*, Google (research gift), **$50,000** (03/2008)
24. co-PI (with Steve Bellovin, Vishal Misra, Henning Schulzrinne, Dan Rubenstein, Nick Maxemchuck), *"Zero Outage Dynamic Intrinsically Assurable Communities (ZODIAC)"*, DARPA/STO, **$835,357** (11/2007 - 05/2009; part of a larger project with Telcordia, Sparta, GMU, and the University of Pennsylvania)
25. PI, *"Travel Supplement under the US/Japan Critical Infrastructure Protection Cooperation Program"*, NSF CyberTrust, **$38,640** (09/2007 - 08/2009)
26. PI, *"PacketSpread: Practical Network Capabilities"*, NSF CyberTrust, CNS-07-14277, **$280,000** (09/2007 - 08/2010)
27. PI, *"Integrated Enterprise Security Management"*, NSF CyberTrust, CNS-07-14647, **$286,486** (08/2007 - 07/2009)
28. PI, *"Safe Browsing Through Web-based Application Communities"*, NY State/Polytechnic CAT, **$25,000** (06/2007 - 06/2009)
29. PI, *"MURI: Foundational and Systems Support for Quantitative Trust Management"*, Office of Naval Research (ONR), **$750,000** (05/2007 - 04/2012; part of a larger project with the University of Pennsylvania and Georgia Institute of Technology)
30. PI (co-PIs: Jason Nieh, Sal Stolfo), *"MURI: Autonomic Recovery of Enterprise-Wide Systems After Attack or Failure with Forward Correction"*, Air Force Office of Scientific Research (AFOSR), **$1,368,000** (05/2007 - 04/2012; part of a larger project with GMU and Penn State University)
31. co-PI (with Sal Stolfo), *"Human Behavior, Insider Threat, and Awareness"*, DHS/I3P, **$616,442** (04/2007 - 03/2009)
32. PI (co-PI: Sal Stolfo), *"Safe Browsing Through Web-based Application Communities"*, Google (research gift), **$50,000** (01/2007)
33. PI (co-PI: Sal Stolfo), *"Supplement to Behavior-based Access Control and Communication in MANETs grant"*, DARPA/IPTO and NRO, **$96,627** (09/2006 - 07/2007)
34. PI, *"Secure Overlay Services"*, NY State/Polytechnic CAT, **$10,000** (09/2006 - 06/2007)
35. PI (co-PIs: Gail Kaiser, Sal Stolfo), *"Enabling Collaborative Self-healing Software Systems"*, NSF CyberTrust, CNS-06-27473, $800,000 (09/2006 - 08/2010)
36. PI (co-PI: Sal Stolfo), *"Behavior-based Access Control and Communication in MANETs"*, DARPA/IPTO, **$100,000** (07/2006 - 06/2007)
37. co-PI (with Steve Bellovin and Sal Stolfo), *"Large-Scale System Defense"*, DTO, **$535,555** (07/2006 - 12/2007)
38. PI, *"Active Decoys for Spyware"*, NY State/Polytechnic CAT, **$25,000** (06/2006 - 12/2007)
39. PI, *"Retrofitting A Flow-oriented Paradigm in Commodity Operating Systems for High-*

Performance Computing", NSF CPA, CCF-05-41093, **$378,091** (01/2006 - 12/2008)

40. co-PI (with Jason Nieh, Gail Kaiser), *"Broadening Participation in Research"*, NSF BPC, **$133,565** (09/2005 - 08/2006)
41. PI, *"Secure Overlay Services"*, NY State/Polytechnic CAT, **$12,500** (09/2005 - 06/2006)
42. co-PI (with Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Intel Corp. (research gift), **$75,000** (08/2005)
43. PI, *"Snakeyes"*, New York State Center for Advanced Technology, **$14,999** (07/2005 - 06/2006)
44. PI, *"Self-protecting Software"*, Columbia Science and Technology Ventures (research gift), $65,000 (06/2005 - 09/2005)
45. co-PI (with Gail Kaiser), *"Trustworthy Computing Curriculum Development"*, Microsoft Research (research gift), **$50,000** (12/2004 - 12/2005)
46. co-PI (with Jason Nieh, Gail Kaiser), *"Secure Remote Computing Services"*, NSF ITR, CNS-04-26623, $1,200,000 (09/2004 - 08/2009)
47. PI, *"Secure Overlay Services"*, NY State/Polytechnic CAT, **$12,500** (09/2004 - 06/2005)
48. co-PI (with Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Intel Corp. (research gift), **$90,000** (06/2004)
49. co-PI (with Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Intel Corp. (research gift), **$120,000** (08/2003)
50. PI (co-PIs: Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Cisco Corp. (research gift), **$76,000** (07/2003)
51. co-PI (with Sal Stolfo, Tal Malkin, Vishal Misra), *"Distributed Intrusion Detection Feasibility Study"*, Department of Defense, **$300,000** (03/2003 - 03/2004)
52. PI, *"STRONGMAN"*, DARPA/ATO, **$23,782** (09/2002 - 08/2003; part of a larger project with the University of Pennsylvania)
53. PI, *"POSSE"*, DARPA/ATO, $16,341 (09/2002 - 08/2003; part of a larger project with the University of Pennsylvania)
54. PI, *"GRIDLOCK"*, NSF Trusted Computing, CCR-TC-02-08972, **$207,000** (07/2002 - 06/2005; part of a larger project with the University of Pennsylvania and Yale University)
55. PI (co-PIs: Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Cisco Corp. (research gift), **$70,000** (07/2002)
56. PI (co-PIs: Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, DARPA/ATO, **$695,000** (06/2002 - 05/2004)
57. PI, *"Code Security Analysis Kit (CoSAK)"*, DARPA/ATO, **$37,000** (07/2001 - 06/2003; part of a larger project with Drexel University)

- **Total:** $34,240,062
- **Total as PI:** $20,625,555

Select Invited Talks

- *"Collaborative, Adaptive Software Defense"*, invited talk, ONR Workshop on Host Computer Security, Chicago, IL, October 2010.
- *"Using Decoys to Identify Malicious Insiders"*, invited talk, Computer Science Department, National University of Singapore, Singapore, August 2010.
- *"Behavior-based Access Control in Wired and Wireless Networks"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"MANET Security: Background and Distributed Defense"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Detecting Insider Attackers"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.

- *"Self-healing and Collaborative Software Defenses",* invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Voice over IP: Risks, Threats, and Vulnerabilities",* invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Determining Device Trustworthiness in Heterogeneous Environments",* invited talk, Intel Workshop on Trust Evidence and End-to-end Trust in Heterogeneous Environments, Santa Clara, CA, May 2010.
- *"Moving Code: Instruction Set Randomization",* invited talk, IC Technical Exchange on Moving Target, Washington, DC, April 2010.
- *"Voice over IP: Risks, Threats and Vulnerabilities",* invited talk, AT&T Labs Research, Florham Park, NJ, April 2010.
- *"Voice over IP: Risks, Threats and Vulnerabilities",* keynote talk, 5th International Conference on Information Systems Security (ICISS), Kolkata, India, December 2009.
- *"Voice over IP: Risks, Threats and Vulnerabilities",* Cyber Infrastructure Protection (CIP) Conference, New York, June 2009.
- *"Voice over IP: Risks, Threats and Vulnerabilities",* keynote talk, Applied Cryptography and Network Security (ACNS) Conference, Paris, France, June 2009.
- *"Automatic Software Self-Healing: Present and Future",* keynote talk, European Workshop on Systems Security (EuroSec), Nuremberg, Germany, March 2009.
- *"VAMPIRE Project Overview",* Symantec Research Labs, Culver City, CA, March 2009.
- *"Survey of IMS/VoIP Security Work",* Agence Nationale de Reserche (ANR), Paris, France, February 2009.
- *"Simulating a Global Passive Adversary for Attacking Tor-like Anonymity Systems",* National Institute for Advanced Industrial Science and Technology (AIST), Japan, November 2008.
- *"Denial of Service Attacks and Resilient Overlay Networks",* ENISA-FORTH Summer School on Network & Information Security, Heraklion, Greece, September 2008.
- *"von Neumann and the Current Computer Security Landscape",* Onassis Foundation Lectures in Science, Heraklion, Greece, July 2008.
- *"Simulating a Global Passive Adversary for Attacking Tor-like Anonymity Systems",* Institute of Computer Science/FORTH, Heraklion, Greece, July 2008.
- *"Race to the bottom: Malicious Hardware",* 1st FORWARD Invitational Workshop for Identifying Emerging Threats in Information and Communication Technology Infrastructures, Goteborg, Sweden, April 2008.

Publications

(Student co-authors are underlined.)

Patents

1. *"Microbilling using a trust management system"*
   Matthew A. Blaze, John Ioannidis, and Angelos D. Keromytis. U.S. Patent Number 7,996,325. Issued on August 9th 2011.
2. *"Methods, systems and media for software self-healing"*
   Michael E. Locasto, Angelos D. Keromytis, Salvatore J. Stolfo, Angelos Stavrou, Gabriela Cretu, Stylianos Sidiroglou, Jason Nieh, and Oren Laadan. U.S. Patent Number 7,962,798. Issued on June 14th, 2011.
3. *"Systems and methods for detecting and inhibiting attacks using honeypots"*
   Stylianos Sidiroglou, Angelos D. Keromytis, and Kostas G. Anagnostakis. U.S. Patent Number 7,904,959. Issued on March 8th, 2011.

4. *"Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems"*
   Salvatore J. Stolfo, Angelos D. Keromytis, Vishal Misra, Michael Locasto, and Janak Parekh. U.S. Patent Number 7,784,097. Issued on August 24th, 2010.
5. *"Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems"*
   Salvatore J. Stolfo, Tal Malkin, Angelos D. Keromytis, Vishal Misra, Michael Locasto, and Janak Parekh. U.S. Patent Number 7,779,463. Issued on August 17th, 2010.
6. *"Systems and methods for computing data transmission characteristics of a network path based on single-ended measurements"*
   Angelos D. Keromytis, Sambuddho Chakravarty, and Angelos Stavrou. U.S. Patent Number 7,660,261. Issued on February 9th, 2010.
7. *"Microbilling using a trust management system"*
   Matthew A. Blaze, John Ioannidis, and Angelos D. Keromytis. U.S. Patent Number 7,650,313. Issued on January 19th 2010.
8. *"Methods and systems for repairing applications"*
   Angelos D. Keromytis, Michael E. Locasto, and Stylianos Sidiroglou. U.S. Patent Number 7,490,268. Issued on February 10th 2009.
9. *"System and method for microbilling using a trust management system"*
   Matthew A. Blaze, John Ioannidis, and Angelos D. Keromytis. U.S. Patent Number 6,789,068. Issued on September 7th 2004.
10. *"Secure and reliable bootstrap architecture"*
    William A. Arbaugh, David J. Farber, Angelos D. Keromytis, and Jonathan M. Smith. U.S. Patent Number 6,185,678. Issued on February 6th 2001.

Journal Publications

1. *"A Comprehensive Survey of Voice over IP Security Research"*
   Angelos D. Keromytis. To appear in the *IEEE Communications Surveys and Tutorials.*
2. *"A System for Generating and Injecting Indistinguishable Network Decoys"*
   Brian M. Bowen, Vasileios P. Kemerlis, Pratap Prabhu, Angelos D. Keromytis, and Salvatore J. Stolfo. To appear in the *Journal of Computer Security (JCS).*
3. *"The Efficient Dual Receiver Cryptosystem and Its Applications"*
   Ted Diament, Homin K. Lee, Angelos D. Keromytis, and Moti Yung. In *International Journal of Network Security (IJNS),* vol 13, no. 3, pp. 135 - 151, November 2011.
4. *"On the Infeasibility of Modeling Polymorphic Shellcode: Re-thinking the Role of Learning in Intrusion Detection Systems"*
   Yingbo Song, Michael E. Locasto, Angelos Stavrou, Angelos D. Keromytis, and Salvatore J. Stolfo. In *Machine Learning Journal (MLJ),* vol. 81, no. 2, pp. 179 - 205, November 2010.
5. *"On The General Applicability of Instruction-Set Randomization"*
   Stephen W. Boyd, Gaurav S. Kc, Michael E. Locasto, Angelos D. Keromytis, and Vassilis Prevelakis. In *IEEE Transactions on Dependable and Secure Computing (TDSC),* vol. 7, no. 3, pp. 255 - 270, July - September 2010.
6. *"Shadow Honeypots"*
   Michalis Polychronakis, Periklis Akritidis, Stelios Sidiroglou, Kostas G. Anagnostakis, Angelos D. Keromytis, and Evangelos Markatos. In *International Journal of Computer and*

Network Security (IJCNS), vol. 2, no. 9, pp. 1 - 15, September 2010.

7. *"Ethics in Security Vulnerability Research"*
Andrea M. Matwyshyn, Ang Cui, Salvatore J. Stolfo, and Angelos D. Keromytis. In *IEEE Security & Privacy Magazine,* vol. 8, no. 2, pp. 67 - 72, March/April 2010.
8. *"Voice over IP Security: Research and Practice"*
Angelos D. Keromytis. In *IEEE Security & Privacy Magazine,* vol. 8, no. 2, pp. 76 - 78, March/April 2010.
9. *"A Market-based Bandwidth Charging Framework"*
David Michael Turner, Vassilis Prevelakis, and Angelos D. Keromytis. In *ACM Transactions on Internet Technology (ToIT),* vol. 10, no. 1, pp. 1 - 30, February 2010.
10. *"A Look at VoIP Vulnerabilities"*
Angelos D. Keromytis. In *USENIX ;login: Magazine,* vol. 35, no. 1, pp. 41 - 50, February 2010.
11. *"Designing Host and Network Sensors to Mitigate the Insider Threat"*
Brian M. Bowen, Malek Ben Salem, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. In *IEEE Security & Privacy Magazine,* vol. 7, no. 6, pp. 22 - 29, November/December 2009.
12. *"Elastic Block Ciphers: Method, Security and Instantiations"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In *Springer International Journal of Information Security (IJIS),* vol 8, no. 3, pp. 211 - 231, June 2009.
13. *"On the Deployment of Dynamic Taint Analysis for Application Communities"*
Hyung Chan Kim and Angelos D. Keromytis. In *IEICE Transactions,* vol. E92-D, no. 3, pp. 548 - 551, March 2009.
14. *"Dynamic Trust Management"*
Matt Blaze, Sampath Kannan, Insup Lee, Oleg Sokolsky, Jonathan M. Smith, Angelos D. Keromytis, and Wenke Lee. In *IEEE Computer Magazine,* vol. 42, no. 2, pp. 44 - 52, February 2009.
15. *"Randomized Instruction Sets and Runtime Environments: Past Research and Future Directions"*
Angelos D. Keromytis. In *IEEE Security & Privacy Magazine,* vol. 7, no. 1, pp. 18 - 25, January/February 2009.
16. *"Anonymity in Wireless Broadcast Networks"*
Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Avi Rubin. In *International Journal of Network Security (IJNS),* vol. 8, no. 1, pp. 37 - 51, January 2009.
17. *"Decentralized Access Control in Networked File Systems"*
Stefan Miltchev, Jonathan M. Smith, Vassilis Prevelakis, Angelos D. Keromytis, and Sotiris Ioannidis. In *ACM Computing Surveys,* vol. 40, no. 3, pp. 10:1 - 10:30, August 2008.
18. *"Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation"*
Kostas G. Anagnostakis, Michael Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. In *Springer International Journal of Information Security (IJIS), ISC 2006 Special Issue,* vol.6, no. 6, pp. 361 - 378, October 2007. (Extended version of the ISC 2006 paper.)
19. *"Requirements for Scalable Access Control and Security Management Architectures"*
Angelos D. Keromytis and Jonathan M. Smith. In *ACM Transactions on Internet Technology (ToIT),* vol. 7, no. 2, pp. 1 - 22, May 2007.

20. *"Virtual Private Services: Coordinated Policy Enforcement for Distributed Applications"* Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, Kostas G. Anagnostakis, and Jonathan M. Smith. In *International Journal of Network Security (IJNS),* vol. 4, no. 1, pp. 69 - 80, January 2007.
21. *"Countering DDoS Attacks with Multi-path Overlay Networks"* Angelos Stavrou and Angelos D. Keromytis. In *Information Assurance Technology Analysis Center (IATAC) Information Assurance Newsletter (IAnewsletter),* vol. 9, no. 3, pp. 26 - 30, Winter 2006. *(Invited paper, based on the CCS 2005 paper.)*
22. *"Conversion Functions for Symmetric Key Ciphers"* Debra L. Cook and Angelos D. Keromytis. In *Journal of Information Assurance and Security (JIAS),* vol. 1, no. 2, pp. 119 - 128, June 2006. *(Extended version of the IAS 2005 paper.)*
23. *"Execution Transactions for Defending Against Software Failures: Use and Evaluation"* Stelios Sidiroglou and Angelos D. Keromytis. In *Springer International Journal of Information Security (IJIS),* vol. 5, no. 2, pp. 77 - 91, April 2006. *(Extended version of the ISC 2005 paper.)*
24. *"Worm Propagation Strategies in an IPv6 Internet"* Steven M. Bellovin, Bill Cheswick, and Angelos D. Keromytis. In *USENIX ;login,* vol. 31, no. 1, pp. 70 - 76, February 2006.
25. *"Cryptography As An Operating System Service: A Case Study"* Angelos D. Keromytis, Theo de Raadt, Jason Wright, and Matthew Burnside. In *ACM Transactions on Computer Systems (ToCS),* vol. 24, no. 1, pp. 1 - 38, February 2006. *(Extended version of USENIX Technical 2003 paper.)*
26. *"Countering Network Worms Through Automatic Patch Generation"* Stelios Sidiroglou and Angelos D. Keromytis. In *IEEE Security & Privacy,* vol. 3, no. 6, pp. 41 - 49, November/December 2005.
27. *"WebSOS: An Overlay-based System For Protecting Web Servers From Denial of Service Attacks"* Angelos Stavrou, Debra L. Cook, William G. Morein, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In *Elsevier Journal of Computer Networks, special issue on Web and Network Security,* vol. 48, no. 5, pp. 781 - 807, August 2005. *(Extended version of the CCS 2003 paper.)*
28. *"Hardware Support For Self-Healing Software Services"* Stelios Sidiroglou, Michael E. Locasto, and Angelos D. Keromytis. In *ACM SIGARCH Computer Architecture News, Special Issue on Workshop on Architectural Support for Security and Anti-Virus (WASSA),* vol. 33, no. 1, pp. 42 - 47, March 2005. Also appeared in the Proceedings of the *Workshop on Architectural Support for Security and Anti-Virus (WASSA),* held in conjunction with the *11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-XI),* pp. 37 - 43. October 2004, Boston, MA.
29. *"The Case For Crypto Protocol Awareness Inside The OS Kernel"* Matthew Burnside and Angelos D. Keromytis. In *ACM SIGARCH Computer Architecture News, Special Issue on Workshop on Architectural Support for Security and Anti-Virus (WASSA),* vol. 33, no. 1, pp. 58 - 64, March 2005. Also appeared in the Proceedings of the

Workshop on Architectural Support for Security and Anti-Virus (WASSA), held in conjunction with the *11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-XI),* pp. 54 - 60. October 2004, Boston, MA.

30. *"Patch-on-Demand Saves Even More Time?"*
Angelos D. Keromytis. In *IEEE Computer*, vol. 37, no. 8, pp. 94 - 96, August 2004.
31. *"Just Fast Keying: Key Agreement In A Hostile Internet"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. In *ACM Transactions on Information and System Security (TISSEC),* vol. 7, no. 2, pp. 1 - 32, May 2004. *(Extended version of the CCS 2002 paper.)*
32. *"SOS: An Architecture for Mitigating DDoS Attacks"*
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In *IEEE Journal on Selected Areas in Communications (JSAC), special issue on Recent Advances in Service Overlay Networks,* vol. 22, no. 1, pp. 176 - 188, January 2004. *(Extended version of the SIGCOMM 2002 paper.)*
33. *"A Secure PLAN"*
Michael Hicks, Angelos D. Keromytis, and Jonathan M. Smith. In *IEEE Transactions on Systems, Man, and Cybernetics (T-SMC) Part C: Applications and Reviews, Special issue on technologies promoting computational intelligence, openness and programmability in networks and Internet services: Part I,* vol. 33, no. 3, pp. 413 - 426, August 2003. *(Extended version of the DANCE 2002 paper.)*
34. *"Drop-in Security for Distributed and Portable Computing Elements"*
Vassilis Prevelakis and Angelos D. Keromytis. In MCB Press *Emerald Journal of Internet Research: Electronic Networking, Applications and Policy,* vol. 13, no. 2, pp. 107 - 115, 2003. *(Extended version of the INC 2002 paper.)*
35. *"Trust Management for IPsec"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In *ACM Transactions on Information and System Security (TISSEC),* vol. 5, no. 2, pp. 1 - 24, May 2002. *(Extended version of the NDSS 2001 paper.)*
36. *"The Price of Safety in an Active Network"*
D. Scott Alexander, Paul B. Menage, Angelos D. Keromytis, William A. Arbaugh, Kostas G. Anagnostakis, and Jonathan M. Smith. In *Journal of Communications and Networks (JCN), special issue on programmable switches and routers,* vol. 3, no. 1, pp. 4 - 18, March 2001. Older versions are available as *University of Pennsylvania Technical Report MS-CIS-99-04* and *University of Pennsylvania Technical Report MS-CIS-98-02.*
37. *"Secure Quality of Service Handling (SQoSH)"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, Steve Muir, and Jonathan M. Smith. In *IEEE Communications Magazine,* vol. 38, no. 4, pp. 106 - 112, April 2000. An older version is available as *University of Pennsylvania Technical Report MS-CIS-99-05.*
38. *"Safety and Security of Programmable Network Infrastructures"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In *IEEE Communications Magazine, issue on Programmable Networks,* vol. 36, no. 10, pp. 84 - 92, October 1998.

39. *"A Secure Active Network Environment Architecture"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In *IEEE Network Magazine, special issue on Active and Controllable Networks,* vol. 12, no. 3, pp. 37 - 45, May/June 1998.
40. *"The SwitchWare Active Network Architecture"*
D. Scott Alexander, William A. Arbaugh, Michael Hicks, Pankaj Kakkar, Angelos D. Keromytis, Jonathan T. Moore, Carl A. Gunter, Scott M. Nettles, and Jonathan M. Smith. In *IEEE Network Magazine, special issue on Active and Programmable Networks,* vol. 12, no. 3, pp. 29 - 36, May/June 1998.

Peer-Reviewed Conference Proceedings

1. *"A Multilayer Overlay Network Architecture for Enhancing IP Services Availability Against DoS"*
Dimitris Geneiatakis, Georgios Portokalidis, and Angelos D. Keromytis. To appear in the Proceedings of the *7th International Conference on Information Systems Security (ICISS).* December 2011, Kolkata, India. *(Acceptance rate: 22.8%)*
2. *"ROP Payload Detection Using Speculative Code Execution"*
Michalis Polychronakis and Angelos D. Keromytis. To appear in the Proceedings of the *6th International Conference on Malicious and Unwanted Software (MALWARE).* October 2011, Fajardo, PR.
3. *"Detecting Traffic Snooping in Tor Using Decoys"*
Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. To appear in Proceedings of the *14th International Symposium on Recent Advances in Intrusion Detection (RAID).* September 2011, Menlo Park, CA. *(Acceptance rate: 23%)*
4. *"Measuring the Deployment Hiccups of DNSSEC"*
Vasilis Pappas and Angelos D. Keromytis. In Proceedings of the *International Conference on Advances in Computing and Communications (ACC), Part III,* pp. 44 - 54. July 2011, Kochi, India. *(Acceptance rate: 39%)*
5. *"Misuse Detection in Consent-based Networks"*
Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *9th International Conference on Applied Cryptography and Network Security (ACNS),* pp. 38 - 56. June 2011, Malaga, Spain. *(Acceptance rate: 18%)*
6. *"Retrofitting Security in COTS Software with Binary Rewriting"*
Padraig O'Sullivan, Kapil Anand, Aparna Kothan, Matthew Smithson, Rajeev Barua, and Angelos D. Keromytis. In Proceedings of the *26th IFIP International Information Security Conference (SEC),* pp. 154 - 172. June 2011, Lucerne, Switzerland. *(Acceptance rate: 24%)*
7. *"Fast and Practical Instruction-Set Randomization for Commodity Systems"*
Georgios Portokalidis and Angelos D. Keromytis. In Proceedings of the *26th Annual Computer Security Applications Conference (ACSAC),* pp. 41 - 48. December 2010, Austin, TX. *(Acceptance rate: 17%)*
8. *"An Adversarial Evaluation of Network Signaling and Control Mechanisms"*
Kangkook Jee, Stelios Sidiroglou-Douskos, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *13th International Conference on Information Security and Cryptology*

(ICISC). December 2010, Seoul, Korea.

9. *"Evaluation of a Spyware Detection System using Thin Client Computing"*
   Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis. In Proceedings of the *13th International Conference on Information Security and Cryptology (ICISC),* pp. 222 - 232. December 2010, Seoul, Korea.
10. *"Crimeware Swindling without Virtual Machines"*
    Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis. In Proceedings of the *13th Information Security Conference (ISC),* pp. 196 - 202. October 2010, Boca Raton, FL. *(Acceptance rate: 27.6%)*
11. *"iLeak: A Lightweight System for Detecting Inadvertent Information Leaks"*
    Vasileios P. Kemerlis, Vasilis Pappas, Georgios Portokalidis, and Angelos D. Keromytis. In Proceedings of the *6th European Conference on Computer Network Defense (EC2ND),* pp. 21 - 28. October 2010, Berlin, Germany.
12. *"Traffic Analysis Against Low-Latency Anonymity Networks Using Available Bandwidth Estimation"*
    Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *15th European Symposium on Research in Computer Security (ESORICS),* pp. 249 - 267. September 2010, Athens, Greece. *(Acceptance rate: 20%)*
13. *"BotSwindler: Tamper Resistant Injection of Believable Decoys in VM-Based Hosts for Crimeware Detection"*
    Brian M. Bowen, Pratap Prabhu, Vasileios P. Kemerlis, Stelios Sidiroglou, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 118 - 137. September 2010, Ottawa, Canada. *(Acceptance rate: 23.5%)*
14. *"An Analysis of Rogue AV Campaigns"*
    Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. In Proceedings of the *13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 442 - 463. September 2010, Ottawa, Canada. *(Acceptance rate: 23.5%)*
15. *"DIPLOMA: Distributed Policy Enforcement Architecture for MANETs"*
    Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *4th International Conference on Network and System Security (NSS)*, pp. 89 - 98. September 2010, Melbourne, Australia. *(Acceptance rate: 26%)*
16. *"Automating the Injection of Believable Decoys to Detect Snooping" (Short Paper)*
    Brian M. Bowen, Vasileios Kemerlis, Pratap Prabhu, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *3rd ACM Conference on Wireless Network Security (WiSec),* pp. 81 - 86. March 2010, Hoboken, NJ. *(Acceptance rate: 21%)*
17. *"BARTER: Behavior Profile Exchange for Behavior-Based Admission and Access Control in MANETs"*
    Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *5th International Conference on Information Systems Security (ICISS),* pp. 193 - 207. December 2009, Kolkata, India. *(Acceptance rate: 19.8%)*
18. *"A Survey of Voice Over IP Security Research"*
    Angelos D. Keromytis. In Proceedings of the *5th International Conference on Information Systems Security (ICISS),* pp. 1 - 17. December 2009, Kolkata, India. *(Invited paper)*

19. *"A Network Access Control Mechanism Based on Behavior Profiles"*
Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *25th Annual Computer Security Applications Conference (ACSAC),* pp. 3 - 12. December 2009, Honolulu, HI. *(Acceptance rate: 20%)*
20. *"Gone Rogue: An Analysis of Rogue Security Software Campaigns"*
Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. In Proceedings of the *5th European Conference on Computer Network Defense (EC2ND),* pp. 1 - 3. November 2009, Milan, Italy. *(Invited paper)*
21. *"Baiting Inside Attackers Using Decoy Documents"*
Brian M. Bowen, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *5th International ICST Conference on Security and Privacy in Communication Networks (SecureComm),* pp. 51 - 70. September 2009, Athens, Greece. *(Acceptance rate: 25.3%)*
22. *"Deny-by-Default Distributed Security Policy Enforcement in Mobile Ad Hoc Networks (Short Paper)"*
Mansoor Alicherry, Angelos D. Keromytis, and Angelos Stavrou. In Proceedings of the *5th International ICST Conference on Security and Privacy in Communication Networks (SecureComm),* pp. 41 - 50. September 2009, Athens, Greece. *(Acceptance rate: 34.7%)*
23. *"Adding Trust to P2P Distribution of Paid Content"*
Alex Sherman, Angelos Stavrou, Jason Nieh, Angelos D. Keromytis, and Clifford Stein. In Proceedings of the *12th Information Security Conference (ISC),* pp. 459 - 474. September 2009, Pisa, Italy. *(Acceptance rate: 27.6%)*
24. *"A2M: Access-Assured Mobile Desktop Computing"*
Angelos Stavrou, Ricardo A. Baratto, Angelos D. Keromytis, and Jason Nieh. In Proceedings of the *12th Information Security Conference (ISC),* pp. 186 - 201. September 2009, Pisa, Italy. *(Acceptance rate: 27.6%)*
25. *"F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *12th Information Security Conference (ISC),* pp. 491 - 506. September 2009, Pisa, Italy. *(Acceptance rate: 27.6%)*
26. *"DoubleCheck: Multi-path Verification Against Man-in-the-Middle Attacks"*
Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *IEEE Symposium on Computers and Communications (ISCC),* pp. 557 - 563. July 2009, Sousse, Tunisia. *(Acceptance rate: 36%)*
27. *"Voice over IP: Risks, Threats and Vulnerabilities"*
Angelos D. Keromytis. In Proceedings (electronic) of the *Cyber Infrastructure Protection (CIP) Conference.* June 2009, New York, NY. *(Invited paper)*
28. *"Capturing Information Flow with Concatenated Dynamic Taint Analysis"*
Hyung Chan Kim, Angelos D. Keromytis, Michael Covington, and Ravi Sahita. In Proceedings of the *4th International Conference on Availability, Reliability and Security (ARES),* pp. 355 - 362. March 2009, Fukuoka, Japan. *(Acceptance rate: 25%)*
29. *"ASSURE: Automatic Software Self-healing Using REscue points"*
Stelios Sidiroglou, Oren Laadan, Nico Viennot, Carlos-René Pérez, Angelos D. Keromytis,

and Jason Nieh. In Proceedings of the *14th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS),* pp. 37 - 48. March 2009, Washington, DC. *(Acceptance rate: 25.6%)*

30. *"Spectrogram: A Mixture-of-Markov-Chains Model for Anomaly Detection in Web Traffic"* Yingbo Song, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *16th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS),* pp. 121 - 135. February 2009, San Diego, CA. *(Acceptance rate: 11.7%)*
31. *"Constructing Variable-Length PRPs and SPRPs from Fixed-Length PRPs"* Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *4th International Conference on Information Security and Cryptology (Inscrypt),* pp. 157 - 180. December 2008, Beijing, China. *(Acceptance rate: 17.5%)*
32. *"Behavior-Profile Clustering for False Alert Reduction in Anomaly Detection Sensors"* Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *24th Annual Computer Security Applications Conference (ACSAC),* pp. 367 - 376. December 2008, Anaheim, CA. *(Acceptance rate: 24.2%)*
33. *"Authentication on Untrusted Remote Hosts with Public-key Sudo"* Matthew Burnside, Mack Lu, and Angelos D. Keromytis. In Proceedings of the *22nd USENIX Large Installation Systems Administration (LISA) Conference,* pp. 103 - 107. November 2008, San Diego, CA.
34. *"Behavior-Based Network Access Control: A Proof-of-Concept"* Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *11th Information Security Conference (ISC),* pp. 175 - 190. Taipei, Taiwan, September 2008. *(Acceptance rate: 23.9%)*
35. *"Path-based Access Control for Enterprise Networks"* Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *11th Information Security Conference (ISC),* pp. 191 - 203. Taipei, Taiwan, September 2008. *(Acceptance rate: 23.9%)*
36. *"Methods for Linear and Differential Cryptanalysis of Elastic Block Ciphers"* Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *13th Australasian Conference on Information Security and Privacy (ACISP),* pp. 187 - 202. July 2008, Wollongong, Australia.*(Acceptance rate: 29.7%)*
37. *"Pushback for Overlay Networks: Protecting against Malicious Insiders"* Angelos Stavrou, Michael E. Locasto, and Angelos D. Keromytis. In Proceedings of the *6th International Conference on Applied Cryptography and Network Security (ACNS),* pp 39 - 54. June 2008, New York, NY. *(Acceptance rate: 22.9%)*
38. *"Casting out Demons: Sanitizing Training Data for Anomaly Sensors"* Gabriela F. Cretu, Angelos Stavrou, *Michael E. Locasto*, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *IEEE Symposium on Security & Privacy,* pp. 81 - 95. May 2008, Oakland, CA. *(Acceptance rate: 11.2%)*
39. *"Taming the Devil: Techniques for Evaluating Anonymized Network Data"* Scott E. Coull, Charles V. Wright, Angelos D. Keromytis, Fabian Monrose, and Michael K. Reiter. In Proceedings of the *15th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS),* pp. 125 - 135. February 2008, San Diego, CA.

(Acceptance rate: 17.8%)

40. *"SSARES: Secure Searchable Automated Remote Email Storage"*
Adam J. Aviv, Michael E. Locasto, Shaya Potter, and Angelos D. Keromytis. In Proceedings of the *23rd Annual Computer Security Applications Conference (ACSAC),* pp. 129 - 138. December 2007, Miami Beach, FL. *(Acceptance rate: 22%)*
41. *"On the Infeasibility of Modeling Polymorphic Shellcode"*
Yingbo Song, Michael E. Locasto, Angelos Stavrou, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *13th ACM Conference on Computer and Communications Security (CCS),* pp. 541 - 551. October/November 2007, Alexandria, VA. *(Acceptance rate: 18.1%)*
42. *"Defending Against Next Generation Attacks Through Network/Endpoint Collaboration and Interaction"*
Spiros Antonatos, Michael E. Locasto, Stelios Sidiroglou, Angelos D. Keromytis, and Evangelos Markatos. In Proceedings of the *3rd European Conference on Computer Network Defense (EC2ND).* October 2007, Heraclion, Greece. *(Invited paper)*
43. *"Elastic Block Ciphers in Practice: Constructions and Modes of Encryption"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *3rd European Conference on Computer Network Defense (EC2ND).* October 2007, Heraclion, Greece.
44. *"The Security of Elastic Block Ciphers Against Key-Recovery Attacks"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *10th Information Security Conference (ISC),* pp. 89 - 103. Valparaiso, Chile, October 2007. *(Acceptance rate: 25%)*
45. *"Characterizing Self-healing Software Systems"*
Angelos D. Keromytis. In Proceedings of the *4th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS),* pp. 22 - 33. September 2007, St. Petersburg, Russia. *(Invited paper)*
46. *"A Study of Malcode-Bearing Documents"*
Wei-Jen Li, Salvatore J. Stolfo, Angelos Stavrou, Elli Androulaki, and Angelos D. Keromytis. In Proceedings of the *4th GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA),* pp. 231 - 250. July 2007, Lucerne, Switzerland. *(Acceptance rate: 21%)*
47. *"From STEM to SEAD: Speculative Execution for Automated Defense"*
Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference,* pp. 219 - 232. June 2007, Santa Clara, CA. *(Acceptance rate: 18.75%)*
48. *"Using Rescue Points to Navigate Software Recovery (Short Paper)"*
Stelios Sidiroglou, Oren Laadan, Angelos D. Keromytis, and Jason Nieh. In Proceedings of the *IEEE Symposium on Security & Privacy,* pp. 273 - 278. May 2007, Oakland, CA. *(Acceptance rate: 8.3%)*
49. *"Mediated Overlay Services (MOSES): Network Security as a Composable Service"*
Stelios Sidiroglou, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *IEEE Sarnoff Symposium.* May 2007, Princeton, NJ. *(Invited paper)*
50. *"Elastic Block Ciphers: The Basic Design"*

Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *2nd ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS),* pp. 350 - 355. March 2007, Singapore.

51. *"Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation"*
Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *9th Information Security Conference (ISC),* pp. 427 - 442. August/September 2006, Samos, Greece. *(Acceptance rate: 20.2%)*
52. *"Low Latency Anonymity with Mix Rings"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *9th Information Security Conference (ISC),* pp. 32 - 45. August/September 2006, Samos, Greece. *(Acceptance rate: 20.2%)*
53. *"W3Bcrypt: Encryption as a Stylesheet"*
Angelos Stavrou, Michael E. Locasto, and Angelos D. Keromytis. In Proceedings of the *4th International Conference on Applied Cryptography and Network Security (ACNS),* pp. 349 - 364. June 2006, Singapore.
54. *"Software Self-Healing Using Collaborative Application Communities"*
Michael E. Locasto, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings of the *13th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS),* pp. 95 - 106. February 2006, San Diego, CA. *(Acceptance rate: 13.6%)*
55. *"Remotely Keyed Cryptographics: Secure Remote Display Access Using (Mostly) Untrusted Hardware"*
Debra L. Cook, Ricardo A. Baratto, and Angelos D. Keromytis. In Proceedings of the *7th International Conference on Information and Communications Security (ICICS),* pp. 363 - 375. December 2005, Beijing, China. *(Acceptance rate: 17.4%)*
56. *"e-NeXSh: Achieving an Effectively Non-Executable Stack and Heap via System-Call Policing"*
Gaurav S. Kc and Angelos D. Keromytis. In Proceedings of the *21st Annual Computer Security Applications Conference (ACSAC),* pp. 259 - 273. December 2005, Tucson, AZ. *(Acceptance rate: 19.6%)*
57. *"Action Amplification: A New Approach To Scalable Administration"*
Kostas G. Anagnostakis and Angelos D. Keromytis. In Proceedings of the *13th IEEE International Conference on Networks (ICON),* vol. 2, pp. 862 - 867. November 2005, Kuala Lumpur, Malaysia.
58. *"A Repeater Encryption Unit for IPv4 and IPv6"*
Norimitsu Nagashima and Angelos D. Keromytis. In Proceedings of the *13th IEEE International Conference on Networks (ICON),* vol. 1, pp. 335 - 340. November 2005, Kuala Lumpur, Malaysia.
59. *"Countering DoS Attacks With Stateless Multipath Overlays"*
Angelos Stavrou and Angelos D. Keromytis. In Proceedings of the *12th ACM Conference on Computer and Communications Security (CCS),* pp. 249 - 259. November 2005, Alexandria, VA. *(Acceptance rate: 15.2%)*
60. *"A Dynamic Mechanism for Recovering from Buffer Overflow Attacks"*
Stelios Sidiroglou, Giannis Giovanidis, and Angelos D. Keromytis. In Proceedings of the *8th*

Information Security Conference (ISC), pp. 1 - 15. September 2005, Singapore. *(Acceptance rate: 14%)*

61. *"gore: Routing-Assisted Defense Against DDoS Attacks"*
Stephen T. Chou, Angelos Stavrou, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *8th Information Security Conference (ISC),* pp. 179 - 193. September 2005, Singapore. *(Acceptance rate: 14%)*
62. *"FLIPS: Hybrid Adaptive Intrusion Prevention"*
Michael E. Locasto, Ke Wang, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *8th International Symposium on Recent Advances in Intrusion Detection (RAID),* pp. 82 - 101. September 2005, Seattle, WA. *(Acceptance rate: 20.4%)*
63. *"Detecting Targeted Attacks Using Shadow Honeypots"*
Kostas G. Anagnostakis, Stelios Sidiroglou, Periklis Akritidis, Konstantinos Xinidis, Evangelos Markatos, and Angelos D. Keromytis. In Proceedings of the *14th USENIX Security Symposium,* pp. 129 - 144. August 2005, Baltimore, MD. *(Acceptance rate: 14%)*
64. *"The Bandwidth Exchange Architecture"*
David Michael Turner, Vassilis Prevelakis, and Angelos D. Keromytis. In Proceedings of the *10th IEEE Symposium on Computers and Communications (ISCC),* pp. 939 - 944. June 2005, Cartagena, Spain.
65. *"An Email Worm Vaccine Architecture"*
Stelios Sidiroglou, John Ioannidis, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *1st Information Security Practice and Experience Conference (ISPEC),* pp. 97 - 108. April 2005, Singapore.
66. *"Building a Reactive Immune System for Software Services"*
Stelios Sidiroglou, Michael E. Locasto, Stephen W. Boyd, and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference,* pp. 149 - 161. April 2005, Anaheim, CA. *(Acceptance rate: 20.3%)*
67. *"Conversion and Proxy Functions for Symmetric Key Ciphers"*
Debra L. Cook and Angelos D. Keromytis. In Proceedings of the *IEEE International Conference on Information Technology: Coding and Computing (ITCC), Information and Security (IAS) Track,* pp. 662 - 667. April 2005, Las Vegas, NV.
68. *"The Effect of DNS Delays on Worm Propagation in an IPv6 Internet"*
Abhinav Kamra, Hanhua Feng, Vishal Misra, and Angelos D. Keromytis. In Proceedings of *IEEE INFOCOM,* vol. 4, pp. 2405 - 2414. March 2005, Miami, FL. *(Acceptance rate: 17%)*
69. *"MOVE: An End-to-End Solution To Network Denial of Service"*
Angelos Stavrou, Angelos D. Keromytis, Jason Nieh, Vishal Misra, and Dan Rubenstein. In Proceedings of the *12th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS),* pp. 81 - 96. February 2005, San Diego, CA. *(Acceptance rate: 12.9%)*
70. *"CryptoGraphics: Secret Key Cryptography Using Graphics Cards"*
Debra L. Cook, John Ioannidis, Angelos D. Keromytis, and Jake Luck. In Proceedings of the *RSA Conference, Cryptographer's Track (CT-RSA),* pp. 334 - 350. February 2005, San Francisco, CA.
71. *"The Dual Receiver Cryptogram and Its Applications"*

Ted Diament, Homin K. Lee, Angelos D. Keromytis, and Moti Yung. In Proceedings of the *11th ACM Conference on Computer and Communications Security (CCS),* pp. 330 - 343. October 2004, Washington, DC. *(Acceptance rate: 13.9%)*

72. *"Hydan: Hiding Information in Program Binaries"*
Rakan El-Khalil and Angelos D. Keromytis. In Proceedings of the *6th International Conference on Information and Communications Security (ICICS),* pp. 187 - 199. October 2004, Malaga, Spain. *(Acceptance rate: 16.9%)*
73. *"Recursive Sandboxes: Extending Systrace To Empower Applications"*
Aleksey Kurchuk and Angelos D. Keromytis. In Proceedings of the *19th IFIP International Information Security Conference (SEC),* pp. 473 - 487. August 2004, Toulouse, France. *(Acceptance rate: 22%)*
74. *"SQLrand: Preventing SQL Injection Attacks"*
Stephen W. Boyd and Angelos D. Keromytis. In Proceedings of the *2nd International Conference on Applied Cryptography and Network Security (ACNS),* pp. 292 - 302. June 2004, Yellow Mountain, China. *(Acceptance rate: 12.1%)*
75. *"CamouflageFS: Increasing the Effective Key Length in Cryptographic Filesystems on the Cheap"*
Michael E. Locasto and Angelos D. Keromytis. In Proceedings of the *2nd International Conference on Applied Cryptography and Network Security (ACNS),* pp. 1 - 15. June 2004, Yellow Mountain, China. *(Acceptance rate: 12.1%)*
76. *"A Pay-per-Use DoS Protection Mechanism For The Web"*
Angelos Stavrou, John Ioannidis, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *2nd International Conference on Applied Cryptography and Network Security (ACNS),* pp. 120 - 134. June 2004, Yellow Mountain, China. *(Acceptance rate: 12.1%)*
77. *"Dealing with System Monocultures"*
Angelos D. Keromytis and Vassilis Prevelakis. In Proceedings (electronic) of the *NATO Information Systems Technology (IST) Panel Symposium on Adaptive Defense in Unclassified Networks.* April 2004, Toulouse, France.
78. *"Managing Access Control in Large Scale Heterogeneous Networks"*
Angelos D. Keromytis, Kostas G. Anagnostakis, Sotiris Ioannidis, Michael Greenwald, and Jonathan M. Smith. In Proceedings (electronic) of the *NATO NC3A Symposium on Interoperable Networks for Secure Communications (INSC).* November 2003, The Hague, Netherlands.
79. *"Countering Code-Injection Attacks With Instruction-Set Randomization"*
Gaurav S. Kc, Angelos D. Keromytis, and Vassilis Prevelakis. In Proceedings of the *10th ACM International Conference on Computer and Communications Security (CCS),* pp. 272 - 280. October 2003, Washington, DC. *(Acceptance rate: 13.8%)*
80. *"Using Graphic Turing Tests to Counter Automated DDoS Attacks Against Web Servers"*
William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *10th ACM International Conference on Computer and Communications Security (CCS),* pp. 8 - 19. October 2003, Washington, DC. *(Acceptance rate: 13.8%)*

81. *"EasyVPN: IPsec Remote Access Made Easy"*
Mark C. Benvenuto and Angelos D. Keromytis. In Proceedings of the *17th USENIX Large Installation Systems Administration (LISA) Conference,* pp. 87 - 93. October 2003, San Diego, CA. *(Acceptance rate: 25%)*
82. *"A Cooperative Immunization System for an Untrusting Internet"*
Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, Angelos D. Keromytis, and Dekai Li. In Proceedings of the *11th IEEE International Conference on Networks (ICON),* pp. 403 - 408. September/October 2003, Sydney, Australia.
83. *"Accelerating Application-Level Security Protocols"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *11th IEEE International Conference on Networks (ICON),* pp. 313 - 318. September/October 2003, Sydney, Australia.
84. *"WebSOS: Protecting Web Servers From DDoS Attacks"*
Debra L. Cook, William G. Morein, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *11th IEEE International Conference on Networks (ICON),* pp. 455 - 460. September/October 2003, Sydney, Australia.
85. *"TAPI: Transactions for Accessing Public Infrastructure"*
Matt Blaze, John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, Pekka Nikander, and Vassilis Prevelakis. In Proceedings of the *8th IFIP Personal Wireless Communications (PWC) Conference,* pp. 90 - 100. September 2003, Venice, Italy.
86. *"Tagging Data In The Network Stack: mbuf_tags"*
Angelos D. Keromytis. In Proceedings of the *USENIX BSD Conference (BSDCon),* pp. 125 - 131. September 2003, San Mateo, CA.
87. *"The Design of the OpenBSD Cryptographic Framework"*
Angelos D. Keromytis, Jason L. Wright, and Theo de Raadt. In Proceedings of the *USENIX Annual Technical Conference,* pp. 181 - 196. June 2003, San Antonio, TX. *(Acceptance rate: 23%)*
88. *"Secure and Flexible Global File Sharing"*
Stefan Miltchev, Vassilis Prevelakis, Sotiris Ioannidis, John Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track,* pp. 165 - 178. June 2003, San Antonio, TX.
89. *"Experience with the KeyNote Trust Management System: Applications and Future Directions"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *1st International Conference on Trust Management,* pp. 284 - 300. May 2003, Heraclion, Greece.
90. *"The STRONGMAN Architecture"*
Angelos D. Keromytis, Sotiris Ioannidis, Michael B. Greenwald, and Jonathan M. Smith. In Proceedings of the *3rd DARPA Information Survivability Conference and Exposition (DISCEX III),* volume 1, pp. 178 - 188. April 2003, Washington, DC.
91. *"Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. In Proceedings of the *9th ACM International Conference on Computer and Communications Security (CCS),* pp. 48 - 58. November 2002, Washington,

DC. *(Acceptance rate: 17.6%)*

92. *"Secure Overlay Services"*
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *ACM SIGCOMM Conference,* pp. 61 - 72. August 2002, Pittsburgh, PA. Also available through the *ACM Computer Communications Review (SIGCOMM Proceedings),* vol. 32, no. 4, October 2002. *(Acceptance rate: 8.3%)*

93. *"Using Overlays to Improve Network Security"*
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *ITCom Conference,* special track on *Scalability and Traffic Control in IP Networks,* pp. 245 - 254. July/August 2002, Boston, MA. *(Invited paper)*

94. *"Designing an Embedded Firewall/VPN Gatweway"*
Vassilis Prevelakis and Angelos D. Keromytis. In Proceedings of the *International Network Conference (INC),* pp. 313 - 322. July 2002, Plymouth, England. **(Best Paper Award)**

95. *"A Study of the Relative Costs of Network Security Protocols"*
Stefan Miltchev, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track,* pp. 41 - 48. June 2002, Monterey, CA.

96. *"A Secure Plan (Extended Version)"*
Michael W. Hicks, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *DARPA Active Networks Conference and Exposition (DANCE),* pp. 224 - 237. May 2002, San Francisco, CA. *(Extended version of the paper IWAN 1999 paper.)*

97. *"Fileteller: Paying and Getting Paid for File Storage"*
John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, and Vassilis Prevelakis. In Proceedings of the *6th Financial Cryptography (FC) Conference,* pp. 282 - 299. March 2002, Bermuda. *(Acceptance rate: 25.6%)*

98. *"Offline Micropayments without Trusted Hardware"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *5th Financial Cryptography (FC) Conference,* pp. 21 - 40. February 2001, Cayman Islands.

99. *"Trust Management for IPsec"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *8th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS)*, pp. 139 - 151. February 2001, San Diego, CA. *(Acceptance rate: 24%)*

100. *"Implementing a Distributed Firewall"*
Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith. In Proceedings of the *7th ACM International Conference on Computer and Communications Security (CCS),* pp. 190 - 199. November 2000, Athens, Greece. *(Acceptance rate: 21.4%)*

101. *"Implementing Internet Key Exchange (IKE)"*
Niklas Hallqvist and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track,* pp. 201 - 214. June 2000, San Diego, CA.

102. *"Transparent Network Security Policy Enforcement"*
Angelos D. Keromytis and Jason Wright. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track,* pp. 215 - 226. June 2000, San Diego, CA.

103. *"Cryptography in OpenBSD: An Overview"*
Theo de Raadt, Niklas Hallqvist, Artur Grabowski, Angelos D. Keromytis, and Niels Provos.

In Proceedings of the *USENIX Annual Technical Conference, Freenix Track,* pp. 93 - 101. June 1999, Monterey, CA.

104. *"DHCP++: Applying an efficient implementation method for fail-stop cryptographic protocols"*
William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *IEEE Global Internet (GlobeCom),* pp. 59 - 65. November 1998, Sydney, Australia.

105. *"Automated Recovery in a Secure Bootstrap Process"*
William A. Arbaugh, Angelos D. Keromytis, David J. Farber, and Jonathan M. Smith. In Proceedings of the *5th Internet Society (ISOC) Symposium on Network and Distributed System Security (SNDSS),* pp. 155 - 167. March 1998, San Diego, CA. An older version is available as *University of Pennsylvania Technical Report MS-CIS-97-13.*

106. *"Implementing IPsec"*
Angelos D. Keromytis, John Ioannidis, and Jonathan M. Smith. In Proceedings of the *IEEE Global Internet (GlobeCom),* pp. 1948 - 1952. November 1997, Phoenix, AZ.

Books/Book Chapters

1. *"Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research"*
Angelos D. Keromytis. Springer Briefs, ISBN 978-1-4419-9865-1, April 2011.
2. *"Buffer Overflow Attacks"*
Angelos D. Keromytis. In *Encyclopedia of Cryptography and Security, 2nd Edition*. Springer, 2011.
3. *"Network Bandwidth Denial of Service (DoS)"*
Angelos D. Keromytis. In *Encyclopedia of Cryptography and Security, 2nd Edition*. Springer, 2011.
4. *"Monitoring Technologies for Mitigating Insider Threats"*
Brian M. Bowen, Malek Ben Salem, Angelos D. Keromytis, and Salvatore J. Stolfo. In *Insider Threats in Cyber Security and Beyond*, Matt Bishop, Dieter Gollman, Jeffrey Hunker, and Christian Probst (editors), pp. 197 - 218. Springer, 2010.
5. *"Voice over IP: Risks, Threats, and Vulnerabilities"*
Angelos D. Keromytis. In *Cyber Infrastructure Security*, Tarek Saadawi and Louis Jordan (editors). Strategic Study Institute (SSI), 2010.
6. *Proceedings of the 2008 New Security Paradigms Workshop (NSPW)*
Angelos D. Keromytis, Anil Somayaji, and M. Hossain Heydari (editors).
7. *Proceedings of the 6th International Conference on Applied Cryptography and Network Security (ACNS)*
Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung (editors). Lecture Notes in Computer Science (LNCS). Springer, 2008.
8. *"Insider Attack and Cyber Security: Beyond the Hacker"*
Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclair, and Sean W. Smith (editors). Advances in Information Security Series, ISBN 978-0387773216. Springer, 2008.
9. *Proceedings of the 2007 New Security Paradigms Workshop (NSPW)*
Kostantin Beznosov (Editor), Angelos D. Keromytis (editor), and M. Hossain Heydari (Editor).

10. *"The Case for Self-Healing Software"*
    Angelos D. Keromytis. In *Aspects of Network and Information Security: Proceedings NATO Advanced Studies Institute (ASI) on Network Security and Intrusion Detection, held in Nork, Yerevan, Armenia, October 2006,* E. Haroutunian, E. Kranakis, and E. Shahbazian (editors). IOS Press, 2007. *(By invitation, as part of the NATO ASI on Network Security, October 2005.)*
11. *"Designing Firewalls: A Survey"*
    Angelos D. Keromytis and Vassilis Prevelakis. In *Network Security: Current Status and Future Directions,* Christos Douligeris and Dimitrios N. Serpanos (editors), pp. 33 - 49. Wiley - IEEE Press, April 2007.
12. *"Composite Hybrid Techniques for Defending against Targeted Attacks"*
    Stelios Sidiroglou and Angelos D. Keromytis. In *Malware Detection,* vol. 27 of Advances in Information Security Series, Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang (editors). Springer, October 2006. *(By invitation, as part of the ARO/DHS 2005 Workshop on Malware Detection.)*
13. *"Trusted computing platforms and secure Operating Systems"*
    Angelos D. Keromytis. In *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* Markus Jakobsson and Steven Myers (editors), pp. 387 - 405. Wiley, 2006.
14. *"CryptoGraphics: Exploiting Graphics Cards for Security"*
    Debra Cook and Angelos D. Keromytis. Advances in Information Security Series, ISBN 0-387-29015-X. Springer, 2006.
15. *Proceedings of the 3rd Workshop on Rapid Malcode (WORM)*
    Angelos D. Keromytis (editor). ACM Press, 2005.
16. *Proceedings of the 3rd International Conference on Applied Cryptography and Network Security (ACNS)*
    John Ioannidis, Angelos D. Keromytis, and Moti Yung (editors). Lecture Notes in Computer Science (LNCS) 3531. Springer, 2005.
17. *"Distributed Trust"*
    John Ioannidis and Angelos D. Keromytis. In *Practical Handbook of Internet Computing,* Munindar Singh (editor), pp. 47/1 - 47/16. CRC Press, 2004.
18. *"Experiences Enhancing Open Source Security in the POSSE Project"*
    Jonathan M. Smith, Michael B. Greenwald, Sotiris Ioannidis, Angelos D. Keromytis, Ben Laurie, Douglas Maughan, Dale Rahn, and Jason L. Wright. In *Free/Open Source Software Development,* Stefan Koch (editor), pp. 242 - 257. Idea Group Publishing, 2004. Also re-published in *Global Information Technologies: Concepts, Methodologies, Tools, and Applications,* Felix B. Tan (editor), pp. 1587 - 1598. Idea Group Publishing, 2007.
19. *"STRONGMAN: A Scalable Solution to Trust Management in Networks"*
    Angelos D. Keromytis. Ph.D. Thesis, University of Pennsylvania, November 2001.
20. *"The Role of Trust Management in Distributed Systems Security"*
    Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis. In *Secure Internet Programming: Issues in Distributed and Mobile Object Systems,* Jan Vitek and Christian Jensen (editors), pp. 185 - 210. Springer-Verlag Lecture Notes in Computer Science *State-of-*

the-Art series, 1999.

21. *"Security in Active Networks"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In *Secure Internet Programming: Issues in Distributed and Mobile Object Systems,* Jan Vitek and Christian Jensen (editors), pp. 433 - 451. Springer-Verlag Lecture Notes in Computer Science *State-of-the-Art* series, 1999.

Workshops

1. *"REASSURE: A Self-contained Mechanism for Healing Software Using Rescue Points"*
Georgios Portokalidis and Angelos D. Keromytis. To appear in the Proceedings of the *6th International Workshop on Security (IWSEC).* November 2011, Tokyo, Japan.
2. *"Taint-Exchange: a Generic System for Cross-process and Cross-host Taint Tracking"*
Angeliki Zavou, Georgios Portokalidis, and Angelos D. Keromytis. To appear in the Proceedings of the *6th International Workshop on Security (IWSEC).* November 2011, Tokyo, Japan.
3. *"The MINESTRONE Architecture: Combining Static and Dynamic Analysis Techniques for Software Security"*
Angelos D. Keromytis, Salvatore J. Stolfo, Junfeng Yang, Angelos Stavrou, Anup Ghosh, Dawson Engler, Marc Dacier, Matthew Elder, and Darrell Kienzle. In Proceedings of the *1st Workshop on Systems Security (SysSec).* July 2011, Amsterdam, Netherlands.
4. *"The SPARCHS Project: Hardware Support for Software Security"*
Simha Sethumadhavan, Salvatore J. Stolfo, David August, Angelos D. Keromytis, and Junfeng Yang. In Proceedings of the *1st Workshop on Systems Security (SysSec).* July 2011, Amsterdam, Netherlands.
5. *"Towards a Forensic Analysis for Multimedia Communication Services"*
Dimitris Geneiatakis and Angelos D. Keromytis. In Proceedings of the *7th International Symposium on Frontiers in Networking with Applications (FINA),* pp. 424 - 429. March 2011, Biopolis, Singapore.
6. *"Security Research with Human Subjects: Informed Consent, Risk, and Benefits"*
Maritza Johnson, Steven M. Bellovin, and Angelos D. Keromytis. In Proceedings of the *2nd Workshop on Ethics in Computer Security Research (WECSR).* March 2011, Saint Lucia.
7. *"Global ISR: Toward a Comprehensive Defense Against Unauthorized Code Execution"*
Georgios Portokalidis and Angelos D. Keromytis. In Proceedings of the *ARO Workshop on Moving Target Defense.* October 2010, Fairfax, VA.
8. *"Securing MANET Multicast Using DIPLOMA"*
Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *5th International Workshop on Security (IWSEC),* pp. 232 - 250. November 2010, Kobe, Japan. *(Acceptance rate: 29%)*
9. *"Evaluating a Collaborative Defense Architecture for MANETs"*
Mansoor Alicherry, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings (electronic) of the *IEEE Workshop on Collaborative Security Technologies (CoSec),* pp. 37 - 42. December 2009, Bangalore, India. *(Acceptance rate: 17.2%)*
10. *"Identifying Proxy Nodes in a Tor Anonymization Circuit"*
Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the

2nd Workshop on Security and Privacy in Telecommunications and Information Systems (SePTIS), pp. 633 - 639. December 2008, Bali, Indonesia. *(Acceptance rate: 37.5%)*

11. *"Online Network Forensics for Automatic Repair Validation"*
Michael E. Locasto, Matthew Burnside, and Angelos D. Keromytis. In Proceedings of the *3rd International Workshop on Security (IWSEC),* pp. 136 - 151. November 2008, Kagawa, Japan. *(Acceptance rate: 19.1%)*
12. *"Return Value Predictability for Self-Healing"*
Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *3rd International Workshop on Security (IWSEC),* pp. 152 - 166. November 2008, Kagawa, Japan. *(Acceptance rate: 19.1%)*
13. *"Asynchronous Policy Evaluation and Enforcement"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *2nd Computer Security Architecture Workshop (CSAW),* pp. 45 - 50. October 2008, Fairfax, VA.
14. *"Race to the bottom: Malicious Hardware"*
Angelos D. Keromytis, Simha Sethumadhavan, and Ken Shepard. In Proceedings of the *1st FORWARD Invitational Workshop for Identifying Emerging Threats in Information and Communication Technology Infrastructures.* April 2008, Goteborg, Sweden. *(Invited paper)*
15. *"Arachne: Integrated Enterprise Security Management"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *8th Annual IEEE SMC Information Assurance Workshop (IAW),* pp. 214 - 220. June 2007, West Point, NY.
16. *"Poster Paper: Band-aid Patching"*
Stelios Sidiroglou, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *3rd Workshop on Hot Topics in System Dependability (HotDep),* pp. 102 - 106. June 2007, Edinburgh, UK.
17. *"Data Sanitization: Improving the Forensic Utility of Anomaly Detection Systems"*
Gabriela F. Cretu, Angelos Stavrou, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *3rd Workshop on Hot Topics in System Dependability (HotDep),* pp. 64 - 70. June 2007, Edinburgh, UK.
18. *"Bridging the Network Reservation Gap Using Overlays"*
Angelos Stavrou, David Michael Turner, Angelos D. Keromytis, and Vassilis Prevelakis. In Proceedings of the *1st Workshop on Information Assurance for Middleware Communications (IAMCOM),* pp. 1 - 6. January 2007, Bangalore, India.
19. *"Next Generation Attacks on the Internet"*
Evangelos Markatos and Angelos D. Keromytis. In Proceedings (electronic) of the *EU-US Summit Series on Cyber Trust: Workshop on System Dependability & Security,* pp. 67 - 73. November 2006, Dublin, Ireland. *(Invited paper)*
20. *"Dark Application Communities"*
Michael E. Locasto, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *New Security Paradigms Workshop (NSPW),* pp. 11 - 18. September 2006, Schloss Dagstuhl, Germany.
21. *"Privacy as an Operating System Service"*
Sotiris Ioannidis, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings (electronic) of the *1st Workshop on Hot Topics in Security (HotSec).* July 2006, Vancouver, Canada.

22. *"PalProtect: A Collaborative Security Approach to Comment Spam"*
Benny Wong, Michael E. Locasto, and Angelos D. Keromytis. In Proceedings of the *7th Annual IEEE SMC Information Assurance Workshop (IAW),* pp. 170 - 175. June 2006, West Point, NY.
23. *"Adding a Flow-Oriented Paradigm to Commodity Operating Systems"*
Christian Soviani, Stephen A. Edwards, and Angelos D. Keromytis. In Proceedings of the *Workshop on Interaction between Operating System and Computer Architecture (IOSCA),* held in conjunction with the IEEE International Symposium on Workload Characterization, pp. 1 - 6. October 2005, Austin, TX.
24. *"Speculative Virtual Verification: Policy-Constrained Speculative Execution"*
Michael E. Locasto, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings of the *New Security Paradigms Workshop (NSPW),* pp. 119 - 124. September 2005, Lake Arrowhead, CA.
25. *"Application Communities: Using Monoculture for Dependability"*
Michael E. Locasto, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings of the *1st Workshop on Hot Topics in System Dependability (HotDep),* held in conjunction with the International Conference on Dependable Systems and Networks (DSN), pp. 288 - 292. June 2005, Yokohama, Japan.
26. *"Towards Collaborative Security and P2P Intrusion Detection"*
Michael E. Locasto, Janak Parekh, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *6th Annual IEEE SMC Information Assurance Workshop (IAW),* pp. 333 - 339. June 2005, West Point, NY.
27. *"FlowPuter: A Cluster Architecture Unifying Switch, Server and Storage Processing"*
Alfred V. Aho, Angelos D. Keromytis, Vishal Misra, Jason Nieh, Kenneth A. Ross, and Yechiam Yemini. In Proceedings of the *1st International Workshop on Data Processing and Storage Networking: towards Grid Computing (DPSN),* pp. 2/1 - 2/7. May 2004, Athens, Greece.
28. *"One Class Support Vector Machines for Detecting Anomalous Windows Registry Accesses"*
Katherine Heller, Krysta Svore, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *ICDM Workshop on Data Mining for Computer Security,* held in conjunction with the *3rd International IEEE Conference on Data Mining,* pp. 2 - 9. November 2003, Melbourn, FL.
29. *"A Holistic Approach to Service Survivability"*
Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Salvatore J. Stolfo. In Proceedings of the *1st ACM Workshop on Survivable and Self-Regenerative Systems (SSRS),* held in conjunction with the *10th ACM International Conference on Computer and Communications Security (CCS),* pp. 11 - 22. October 2003, Fairfax, VA.
30. *"High-Speed I/O: The Operating System As A Signalling Mechanism"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *ACM SIGCOMM Workshop on Network-I/O Convergence: Experience, Lessons, Implications (NICELI),* held in conjunction with the *ACM SIGCOMM Conference,* pp. 220 - 227. August 2003, Karlsruhe, Germany.

31. *"A Network Worm Vaccine Architecture"*
Stelios Sidiroglou and Angelos D. Keromytis. In Proceedings of the *12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security,* pp. 220 - 225. June 2003, Linz, Austria.

32. *"Design and Implementation of Virtual Private Services"*
Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security, Special Session on Trust Management in Collaborative Global Computing,* pp. 269 - 274. June 2003, Linz, Austria.

33. *"WebDAVA: An Administrator-Free Approach To Web File-Sharing"*
Alexander Levine, Vassilis Prevelakis, John Ioannidis, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Distributed and Mobile Collaboration,* pp. 59 - 64. June 2003, Linz, Austria.

34. *"Protocols for Anonymity in Wireless Networks"*
Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Avi Rubin. In Proceedings of the *11th International Workshop on Security Protocols.* April 2003, Cambridge, England.

35. *"xPF: Packet Filtering for Low-Cost Network Monitoring"*
Sotiris Ioannidis, Kostas G. Anagnostakis, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *Workshop on High Performance Switching and Routing (HPSR),* pp. 121 - 126. May 2002, Kobe, Japan.

36. *"Toward Understanding the Limits of DDoS Defenses"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *10th International Workshop on Security Protocols,* Springer-Verlag Lecture Notes in Computer Science, vol. 2467. April 2002, Cambridge, England.

37. *"Toward A Unified View of Intrusion Detection and Security Policy"*
Matt Blaze, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *10th International Workshop on Security Protocols,* Springer-Verlag Lecture Notes in Computer Science, vol. 2467. April 2002, Cambridge, England.

38. *"Efficient, DoS-resistant, Secure Key Exchange for Internet Protocols"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. In Proceedings of the *9th International Workshop on Security Protocols,* Springer-Verlag Lecture Notes in Computer Science, vol. 2133, pp. 40 - 48. April 2001, Cambridge, England.

39. *"Scalable Resource Control in Active Networks"*
Kostas G. Anagnostakis, Michael W. Hicks, Sotiris Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *2nd International Workshop for Active Networks (IWAN),* pp. 343 - 357. October 2000, Tokyo, Japan.

40. *"A Secure Plan"*
Michael W. Hicks and Angelos D. Keromytis. In Proceedings of the *1st International Workshop for Active Networks (IWAN),* pp. 307 - 314. June - July 1999, Berlin, Germany. An

extended version is available as *University of Pennsylvania Technical Report MS-CIS-99-14,* and was also published in the Proceedings of the *DARPA Active Networks Conference and Exposition (DANCE),* May 2002.

41. *"Trust Management and Network Layer Security Protocols"*
    Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *7th International Workshop on Security Protocols,* Springer-Verlag Lecture Notes in Computer Science, vol. 1796, pp. 103 - 108. April 1999, Cambridge, England.
42. *"The SwitchWare Active Network Implementation"*
    D. Scott Alexander, Michael W. Hicks, Pankaj Kakkar, Angelos D. Keromytis, Marianne Shaw, Jonathan T. Moore, Carl A. Gunter, Trevor Jim, Scott M. Nettles, and Jonathan M. Smith. In Proceedings of the *ACM SIGPLAN Workshop on ML,* held in conjunction with the *International Conference on Functional Programming (ICFP),* pp. 67 - 76. September 1998, Baltimore, MD.
43. *"KeyNote: Trust Management for Public-Key Infrastructures"*
    Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. In Proceedings of the *6th International Workshop on Security Protocols,* Springer-Verlag Lecture Notes in Computer Science, vol. 1550, pp. 59 - 63. April 1998, Cambridge, England. Also available as *AT&T Technical Report 98.11.1.*

Additional Publications

1. *"Transport Layer Security (TLS) Authorization Using KeyNote"*
   Angelos D. Keromytis. *Request For Comments (RFC) 6042,* October 2010.
2. *"X.509 Key and Signature Encoding for the KeyNote Trust Management System"*
   Angelos D. Keromytis. *Request For Comments (RFC) 5708,* January 2010.
3. *"SSARES: Secure Searchable Automated Remote Email Storage"*
   Adam J. Aviv, Michael E. Locasto, Shaya Potter, and Angelos D. Keromytis. In the Columbia Computer Science Student Research Symposium, Fall 2006.
4. *"IP Security Policy Requirements"*
   Matt Blaze, Angelos D. Keromytis, Michael Richardson, and Luis Sanchez. *Request For Comments (RFC) 3586,* August 2003.
5. *"On the Use of Stream Control Transmission Protocol (SCTP) with IPsec"*
   Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, and Randal R. Stewart. *Request For Comments (RFC) 3554,* June 2003.
6. *"The Use of HMAC-RIPEMD-160-96 within ESP and AH"*
   Angelos D. Keromytis and Niels Provos. *Request For Comments (RFC) 2857,* June 2000.
7. *"DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System"*
   Matt Blaze, John Ioannidis, and Angelos D. Keromytis. *Request For Comments (RFC) 2792,* March 2000.
8. *"The KeyNote Trust-Management System, Version 2"*
   Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis. *Request For Comments (RFC) 2704,* September 1999.

Technical Reports/Works in Progress

1. *"Symantec Report on Rogue Security Software, July 2008 - June 2009"*
   Marc Fossi, Dean Turner, Eric Johnson, Trevor Mack, Teo Adams, Joseph Blackbird, Mo

King Low, David McKinney, Marc Dacier, Angelos D. Keromytis, Corrado Leita, Marco Cova, Jon Orbeton, and Olivier Thonnard. Symantec Technical Report, October 2009.

2. *"LinkWidth: A Method to Measure Link Capacity and Available Bandwidth using Single-End Probes"*
   Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-002-08,* January 2008.
3. *"Can P2P Replace Direct Download for Content Distribution?"*
   Alex Sherman, Angelos Stavrou, Jason Nieh, Cliff Stein, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-020-07,* March 2007.
4. *"A Model for Automatically Repairing Execution Integrity"*
   Michael E. Locasto, Gabriela F. Cretu, Angelos Stavrou, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-005-07,* January 2007.
5. *"Speculative Execution as an Operating System Service"*
   Michael E. Locasto and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-024-06,* May 2006.
6. *"Quantifying Application Behavior Space for Detection and Self-Healing"*
   Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, Angelos D. Keromytis, and Salvatore J. Stolfo. *Columbia University Computer Science Department Technical Report CUCS-017-06,* April 2006.
7. *"Bloodhound: Searching Out Malicious Input in Network Flows for Automatic Repair Validation"*
   Michael E. Locasto, Matthew Burnside, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-016-06,* April 2006.
8. *"Binary-level Function Profiling for Intrusion Detection and Smart Error Virtualization"*
   Michael E. Locasto and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-002-06,* January 2006.
9. *"A General Analysis of the Security of Elastic Block Ciphers"*
   Debra Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-038-05,* September 2005.
10. *"The Pseudorandomness of Elastic Block Ciphers"*
    Debra Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-037-05,* September 2005.
11. *"PachyRand: SQL Randomization for the PostgreSQL JDBC Driver"*
    Michael E. Locasto and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-033-05,* August 2005.
12. *"Elastic Block Ciphers: The Feistel Cipher Case"*
    Debra L. Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-021-04,* May 2004.
13. *"Collaborative Distributed Intrusion Detection"*
    Michael E. Locasto, Janak J. Parekh, Salvatore J. Stolfo, Angelos D. Keromytis, Tal Malkin, and Vishal Misra. *Columbia University Computer Science Department Technical Report CUCS-012-04,* March 2004.

14. *"Elastic Block Ciphers"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-010-04,* February 2004.
15. *"Just Fast Keying (JFK)"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. *IETF IPsec Working Group*, April 2002,.
16. *"CASPER: Compiler-Assisted Securing of Programs at Runtime"*
Gaurav S. Kc, Stephen A. Edwards, Gail E. Kaiser, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-025-02,* 2002.
17. *"The 'suggested ID' extension for IKE"*
Angelos D. Keromytis and William Sommerfeld. *IETF IPsec Working Group*, November 2001.
18. *"SPKI: ShrinkWrap"*
Angelos D. Keromytis and William A. Simpson. *IETF SPKI Working Group*, September 1997.
19. *"Active Network Encapsulation Protocol (ANEP)"*
D. Scott Alexander, Bob Braden, Carl A. Gunter, Alden W. Jackson, Angelos D. Keromytis, Gary J. Minden, and David Wetherall. *Active Networks Group, DARPA Active Networks Project*, August 1997.
20. *"Creating Efficient Fail-Stop Cryptographic Protocols"*
Angelos D. Keromytis and Jonathan M. Smith. *University of Pennsylvania Technical Report MS-CIS-96-32*, December 1996.

Re-Exam

PATENT
Customer No. 23,630
Attorney Docket No. 077580-0160

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U. S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§ 1.933 AND 1.555

Pursuant to 37 C.F.R. §§ 1.933 and 1.555, VirnetX Inc., the patent owner, brings to the attention of the Examiner the documents listed on the attached PTO/SB/08 Form.

Copies of the listed U.S. patent documents are not enclosed. Copies of listed foreign patent documents and non-patent literature documents not previously submitted in a priority application—citation nos. C8, C19, C21, C24, and D257, D258, D259, D261, D263, D264, D266, and D292-D1219—are enclosed. *See* M.P.E.P. § 609.02(B)(2).

The patent owner respectfully requests that the Examiner consider the listed documents and indicate that they were considered by making appropriate notations on the attached form and returning the same to patent owner.

This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art." If the Examiner applies any of the documents as prior art against any claim in the instant proceeding and the patent owner determines that the cited documents do not constitute "prior art" under United States law, the patent owner reserves the right to present to the U.S. Patent and Trademark Office the relevant facts and law regarding the appropriate status of such documents.

The patent owner further reserves the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims in the instant proceeding.

If there is any fee due in connection with the filing of this paper, please charge the fee to Deposit Account 502624.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Dated: September 20, 2012

By: /Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
McDermott Will & Emery LLP
Attorney for Patent Owner

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com

Please recognize our Customer No. 23630 as our correspondence address.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	1	of	52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code *(if known)*			
		A1	09/399,753	09/22/1998	Graig Miller et al.	
		A2	60/151,563	08/31/1999	Bryan Whittles	
		A3	60/134,547	05/17/1999	Victory Sheymov	
		A4	2,895,502	07/21/1959	Roper et al.	
		A5	4,761,334	08/1988	Sagoi et al.	
		A6	4,885,778	12/5/1989	Weiss, Kenneth	
		A7	4,920,484	4/24/1990	Ranade	
		A8	4,933,846	06/12/1990	Humphrey et al.	
		A9	4,952,930	08/28/1990	Franaszek et al.	
		A10	4,988,990	01/29/1991	Warrior	
		A11	5,164,988	11/17/1992	Matyas	
		A12	5,204,961	04/20/1993	Barlow	
		A13	5,276,735	01/04/1994	Boebert et al	
		A14	5,303,302	04/12/1994	Burrows	
		A15	5,311,593	05/10/1994	Carmi	
		A16	5,329,521	07/12/1994	Walsh et al.	
		A17	5,341,426	08/23/1994	Barney et al.	
		A18	5,367,643	11/22/1994	Chang et al	
		A19	5,384,848	01/24/1995	Kikuchi	
		A20	5,511,122	04/23/1996	Atkinson	
		A21	5,548,646	08/20/1996	Aziz et al.	
		A22	5,559,883	09/24/1996	Williams	
		A23	5,561,669	10/01/1996	Lenney et al	
		A24	5,588,060	12/24/1996	Aziz	
		A25	5,590,285	12/31/1996	Krause et al.	
		A26	5,625,626	04/29/1997	Umekita	
		A27	5,629,984	05/13/1997	McManis	
		A28	5,654,695	08/05/1997	Olnowich et al	
		A29	5,682,480	10/28/1997	Nakagawa	
		A30	5,689,566	11/18/1997	Nguyen	
		A31	5,689,641	11/18/1997	Ludwig et al.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	2	of	52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A32	5,740,375	04/14/1998	Dunne et al.	
		A33	5,757,925	05/1998	Faybishenko	
		A34	5,764,906	06/1998	Edelstein et al.	
		A35	5,771,239	06/23/1998	Moroney et al.	
		A36	5,774,660	6/30/1998	Brendel et al	
		A37	5,787,172	07/28/1998	Arnold	
		A38	5,790,548	08/04/1998	Sitaraman et al.	
		A39	5,796,942	08/18/1998	Esbensen	
		A40	5,805,801	09/08/1998	Holloway et al.	
		A41	5,805,803	09/08/1998	Birrell et al.	
		A42	5,822,434	10/13/1998	Caronni et al.	
		A43	5,842,040	11/24/1998	Hughes et al.	
		A44	5,845,091	12/01/1998	Dunne et al.	
		A45	5,864,666	01/1999	Shrader, Theodore Jack London	
		A46	5,867,650	02/02/1998	Osterman	
		A47	5,870,610	02/09/1999	Beyda et al.	
		A48	5,878,231	05/02/1999	Baehr et al	
		A49	5,892,903	04/06/1999	Klaus	
		A50	5,898,830	04/27/1999	Wesinger, Jr. et al.	
		A51	5,905,859	05/18/1999	Holloway et al.	
		A52	5,918,018	06/29/1999	Gooderum et al.	
		A53	5,918,019	06/29/1999	Valencia	
		A54	5,950,195	09/07/1999	Stockwell et al.	
		A55	5,950,519	09/14/1999	Anatoli	
		A56	5,960,204	09/28/1999	Yinger et al.	
		A57	5,996,016	11/30/1999	Thalheimer et al.	
		A58	6,006,259	12/21/1999	Adelman et al.	
		A59	6,006,272	12/21/1999	Aravamudan et al	
		A60	6,016,318	01/18/2000	Tomoike	
		A61	6,016,512	01/18/2000	Huitema	
		A62	6,041,342	03/21/2000	Yamaguchi	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	3	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A63	6,052,788	04/2000	Wesinger et al.	
		A64	6,055,574	04/25/2000	Smorodinsky et al.	
		A65	6,061,346	05/2000	Nordman, Mikael	
		A66	6,061,736	05/09/2000	Rochberger et al	
		A67	6,079,020	06/20/2000	Liu	
		A68	6,081,900	06/2000	Subramaniam et al.	
		A69	6,092,200	07/18/2000	Muniyappa et al.	
		A70	6,101,182	08/2000	Sistanizadeh et al.	
		A71	6,119,171	09/12/2000	Alkhatib	
		A72	6,119,234	09/12/2000	Aziz et al.	
		A73	6,131,121	10/10/2000	Mattaway et al.	
		A74	6,147,976	11/14/2000	Shand et al.	
		A75	6,157,957	12/05/2000	Berthaud	
		A76	6,158,011	12/05/2000	Chen et al.	
		A77	6,168,409	01/02/2001	Fare	
		A78	6,173,399	01/09/2001	Gilbrech	
		A79	6,175,867	01/16/2001	Taghadoss	
		A80	6,178,409	01/23/2001	Weber et al.	
		A81	6,178,505	01/23/2001	Schneider et al	
		A82	6,179,102	01/30/2001	Weber, et al.	
		A83	6,182,141	1/30/2001	Blum et al.	
		A84	6,199,112	03/2001	Wilson, Stephen K.	
		A85	6,202,081	03/2001	Naudus, Stanley T.	
		A86	6,222,842	04/24/2001	Sasyan et al.	
		A87	6,223,287	04/24/2001	Douglas et al.	
		A88	6,226,748	05/01/2001	Bots et al.	
		A89	6,226,751	05/01/2001	Arrow et al..	
		A90	6,233,618	05/15/2001	Shannon	
		A91	6,243,360	06/05/2001	Basilico	
		A92	6,243,749	06/05/2001	Sitaraman et al.	
		A93	6,243,754	06/05/2001	Guerin et al	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	4	of	52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code *(if known)*			
		A94	6,246,670	06/12/2001	Karlsson et al.	
		A95	6,256,671	07/03/2001	Strentzsch et al.	
		A96	6,262,987	07/17/01	Mogul, Jeffrey C.	
		A97	6,263,445	07/17/2001	Blumenau	
		A98	6,269,099	07/31/2001	Borella et al.	
		A99	6,286,047	09/04/2001	Ramanathan et al	
		A100	6,298,341	10/02/01	Mann, et al.	
		A101	6,301,223	10/9/2001	Hrastar et al	
		A102	6,308,213	10/23/2001	Valencia	
		A103	6,308,274	10/23/2001	Swift	
		A104	6,311,207	10/30/2001	Mighdoll et al	
		A105	6,314,463	11/2001	Abbott et al.	
		A106	6,324,161	11/27/2001	Kirch	
		A107	6,330,562	12/11/2001	Boden et al.	
		A108	6,332,158	12/18/2001	Risley et al.	
		A109	6,333,272	12/25/01	McMillin, et al.	
		A110	6,338,082	01/08/02	Schneider, Eric	
		A111	6,353,614	03/05/2002	Borella et al.	
		A112	6,425,003	07/23/2002	Herzog et al.	
		A113	6,430,155	08/06/2002	Davie et al	
		A114	6,430,610	08/06/2002	Carter	
		A115	6,487,598	11/26/2002	Valencia	
		A116	6,496,867	12/17/2002	Beser et al.	
		A117	6,499,108	12/24/2002	Johnson	
		A118	6,502,135	12/2002	Munger et al.	
		A119	6,505,232	01/07/2003	Mighdoll et al	
		A120	6,510,154	01/21/2003	Mayes et al	
		A121	6,549,516	04/15/2003	Albert et al	
		A122	6,557,037	04/2003	Provino, Joseph E.	
		A123	6,560,634	05/06/2003	Broadhurst	
		A124	6,571,296	05/27/2002	Dillon	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 5	of 52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A125	6,571,338	05/27/2003	Shaio et al.	
		A126	6,581,166	7/17/2003	Hirst et al.	
		A127	6,606,708	08/12/2003	Devine et al.	
		A128	6,615,357	9/2/2003	Boden et al.	
		A129	6,618,761	09/09/2003	Munger et al.	
		A130	6,671,702	12/30/2003	Kruglikov et al	
		A131	6,687,551	2/3/2004	Steindl	
		A132	6,687,746	02/03/04	Shuster, et al.	
		A133	6,701,437	03/02/2004	Hoke et al.	
		A134	6,714,970	3/30/2004	Fiveash et al.	
		A135	6,717,949	4/6/2004	Boden et al.	
		A136	6,751,738	06/15/2004	Wesinger, Jr. et al..	
		A137	6,752,166	06/22/04	Lull, et al.	
		A138	6,757,740	06/29/04	Parekh, et al.	
		A139	6,760,766	7/6/2004	Sahlqvist	
		A140	6,813,777	11/2004	Weinberger et al.	
		A141	6,826,616	11/30/2004	Larson et al.	
		A142	6,839,759	1/4/2005	Larson et al.	
		A143	6,937,597	08/30/2005	Rosenberg et al.	
		A144	7,010,604	3/7/2006	Munger et al.	
		A145	7,039,713	05/2006	Van Gunter et al.	
		A146	7,072,964	07/04/2006	Whittle et al.	
		A147	7,133,930	11/7/2006	Munger et al.	
		A148	7,167,904	01/23/07	Devarajan, et al.	
		A149	7,188,175	03/06/07	McKeeth, James A.	
		A150	7,188,180	3/6/2007	Larson et al.	
		A151	7,197,563	3/27/2007	Sheymov et al.	
		A152	7,353,841	04/08/08	Kono, et al.	
		A153	7,418,504	08/2008	Larson et al.	
		A154	7,461,334	12/02/08	Lu, et al.	
		A155	7,490,151	02/2009	Munger et al.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 6	of 52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code *(if known)*			
		A156	7,493,403	02/2009	Shull et al.	
		A157	7,584,500	09/2009	Dillon et al.	
		A158	7,764,231	07/27/2010	Karr et al.	
		A159	7,852,861	12/2010	Wu et al.	
		A160	7,921,211	04/2011	Larson et al.	
		A161	7,933,990	04/2011	Munger et al.	
		A162	8,051,181	11/2011	Larson et al.	

Note: Submission of copies of U.S. Patents and published U.S. Patent Applications is not required.

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	7	of	52	*Attorney Docket Number*	077580-0160

PUBLISHED U.S. PATENT APPLICATIONS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		B1	US2001/0049741	12/2001	Skene et al.	
		B2	US2002/0004898	1/10/02	Droge	
		B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
		B4	US2004/0199493	10/2004	Ruiz et al.	
		B5	US2004/0199520	10/2004	Ruiz et al.	
		B6	US2004/0199608	10/2004	Rechterman et al.	
		B7	US2004/0199620	10/2004	Ruiz et al.	
		B8	US2005/0055306	3/10/05	Miller et al.	
		B9	US2005/0108517	05/2005	Dillon et al.	
		B10	US2006/0059337	03/16/2006	Polyhonen et al.	
		B11	US2006/0123134	06/2006	Munger et al.	
		B12	US2007/0208869	09/2007	Adelman et al.	
		B13	US2007/0214284	09/2007	King et al.	
		B14	US2007/0266141	11/2007	Norton, Michael Anthony	
		B15	US2008/0005792	01/2008	*Larson et al.	
		B16	US2008/0144625	06/2008	Wu et al.	
		B17	US2008/0235507	09/2008	Ishikawa et al.	
		B18	US2009/0193498	07/2009	Agarwal et al.	
		B19	US2009/0193513	07/2009	Agarwal et al.	
		B20	US2009/0199258	08/2009	Deng et al.	
		B21	US2009/0199285	09/2009	Agarwal et al.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	8	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

FOREIGN PATENT DOCUMENTS							
Tab	Examiner Initials*	Cite No.	Foreign Patent Document Country Code Number Kind Code (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Translation
		C1	DE19924575	12/2/99	Provino et al.		
		C2	EP0814589	12/29/1997	AT&T Corp.		
		C3	EP0838930	4/29/1988	Digital Equipment Corporation		
		C4	EP0858189	8/12/98	Maciel et al.		
		C5	EP836306	4/15/1998	HEWLETT PACKARD CO		
		C6	GB2317792	04/01/1998	Secure Computing Corporation		
		C7	GB2334181	08/11/1999	NEC Technologies		
		C8	GB2340702	02/23/2000	Sun Microsystems Inc.		
		C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		
		C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		
		C11	JP10-070531	03/10/1998	Brother Ind Ltd.		
		C12	JP62-214744	9/21/1987	Hitachi Ltd.		
		C13	WO0070458	11/23/2000	Comsec Corporation		
		C14	WO0017775	3/30/00	Miller et al.		
		C15	WO01016766	03/08/2001	Science Applications International Corporation		
		C16	WO0150688	7/12/01	Kriens		
		C17	WO9827783	06/25/1998	Northern Telecom Limited		
		C18	WO9855930	12/10/98	Tang		
		C19	WO9843396	10/01/1998	Northern Telecom Limited		
		C20	WO9859470	12/30/98	Kanter et al.		
		C21	WO9911019	03/04/1999	V One Corp		
		C22	WO9938081	7/29/99	Paulsen et al.		
		C23	WO9948303	9/23/99	Cox et al.		
		C24	WO01/61922	02/12/2001	Science Application International Corporation		

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	9	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D4	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	D6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D8	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D9	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D10	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	D11	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	D12	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D13	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D14	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	D15	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D16	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D17	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	D18	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	D19	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	D20	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D21	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D22	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D23	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	10	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D24	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D25	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	D26	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D27	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conference on Communications architectures & protocols. pp. 84-91, ACM Press, NY, NY 1986.	
	D28	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D29	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	D30	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation.	
	D31	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D32	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D33	I. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) RFC1101, DNS SRV)	
	D34	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	D35	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	D37	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	D38	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	D39	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	D40	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	D41	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	D42	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	D43	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	
	D44	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	*Complete if Known*	
	Control Number	95/001,949
	Filing Date	March 28, 2012
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Dennis G. Bonshock
Sheet 11 of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D45	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	D46	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	D47	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista)	
	D48	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	D49	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	D50	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)	
	D51	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/199706200300312/www.aventail.com/educate/whitepaper/ipmw.html (1997). (Corporate Access, Aventail)	
	D53	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	D54	Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschtag I, Onion Routing)	
	D55	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	D62	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	D63	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	D64	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	***Complete if Known***	
	Control Number	95/001,949
	Filing Date	March 28, 2012
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Dennis G. Bonshock
Sheet 12 of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D65	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Definition, ANX)	
	D66	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	D67	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	
	D68	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	D69	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	D70	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	D71	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	D72	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	D73	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured there from and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	D74	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (*available at* http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue). (NT Beta, Microsoft Prior Art VPN Technology)	
	D76	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	D77	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	D78	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	D79	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	D80	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	D81	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). DISA, SIPRNET)	
	D82	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	D83	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	13	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D84	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	D85	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	D86	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	D87	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	D88	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	D89	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	D90	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	D91	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	D92	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	D93	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	D94	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	D95	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	D96	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	D97	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	D98	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	D99	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*,<draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). Scott VPNs)	
	D101	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	D102	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	D103	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	D104	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	D105	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	14	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D106	Telcordia Technologies, “ANX Release 1 Document Corrections,” AIAG (May 11, 1999). (Telcordia, ANX)	
	D107	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	D108	Bhattacharya, et al., “An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)”, IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	D109	B. Patel, et al. “DHCP Configuration of IPSEC Tunnel Mode,” IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	D110	Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D111	“Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources,” FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	D112	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	D113	MITRE Organization, “Technical Description,” Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	D114	H. Schulzrinne, et al. “Application-Layer Mobility Using SIP,” Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	D115	Kindred et al, “Dynamic VPN Communities: Implementation and Experience,” DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	D116	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	D117	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	D118	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	D119	Assured Digital Products. (Assured Digital)	
	D120	Aventail Corp., “Aventail AutoSOCKS the Client Key to Network Security,” Aventail Corporation White Paper. (Network Security, Aventail)	
	D121	Cindy Moran, “DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet).” (Moran, SIPRNET)	
	D122	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	D123	“Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	D124	*Onion Routing*, “Investigation of Route Selection Algorithms,” *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	D125	Secure Computing, “Bullet-Proofing an Army Net,” Washington Technology. (Secure, SIPRNET)	
	D126	SPARTA “Dynamic Virtual Private Network.” (Sparta, VPN SYSTEMS)	
	D127	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	D128	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	D129	Kaufman et al., “Implementing IPsec,” (Copyright 1999) (Implementing IPsec)	
	D130	Network Associates *Gauntlet Firewall For Unix User’s Guide Version 5.0* (1999). (Gauntlet User’s Guide – Unix, Firewall Products)	
	D131	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Dennis G. Bonshock
Sheet	15	of	52	Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D132	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	D140	Dan Sterne *et al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	D142	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	D143	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	D144	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	D145	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D147	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D148	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D149	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	16	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D150	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, *Essential Winlnet* 313-423 (Addison Wesley Longman 1998) (Essential Winlnet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	D162	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/techneUarchive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	D165	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	D168	Kenneth Gregg, *et al., Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/enus/library/bb545687(VS.85.printer).aspx (Remote Access)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	17	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D170	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D171	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D172	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch0l.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D175	F-Secure, *F-Secure NameSurfer*(May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) F-Secure VPN 3)	
	D177	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	D185	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	18	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D187	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	D189	F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., *SafeNet/Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	D198	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	D204	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	D205	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	D206	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	D207	Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0* (September 21, 1998)	
	D209	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	D210	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	D211	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	D212	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	D213	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	D214	*Virtual Private Network Demonstration* (March 21, 1998)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	19	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D215	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	D216	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	D217	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	D218	Information Assurance, *Science Fair Agenda* (2000)	
	D219	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	D220	*IFE 3.1 Technology Dependencies* (2000)	
	D221	*IFE 3.1 Topology* (February 9, 2000)	
	D222	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	D224	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	D225	Information Assurance/NAI Labs, Dynamic Virtual Private Networks Presentation v.3 (2000)	
	D226	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	D228	Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, *MCSE Test Success: Proxy Server 2*(1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D238	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	D239	*AutoSOCKS v2. 1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers, 1 99x/msg00945.html	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	20	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D241	FirstVPN Enterprise Networks, Overview	
	D242	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	D243	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	D244	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	D245	Virtual Private Networks - Assured Digital Incorporated - ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	D246	Accessware - The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	D247	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	D248	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	D250	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, “Building and Managing Virtual Private Networks” (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, “A novel scheme combining interleaving technique with cipher in Rayleigh fading channels,” Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
	D256	Davies and Price, edited by Tadahiro Uezono, “Network Security”, Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
	D257	Davies et al., “An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,” Security for Computer Networks, Second Edition, pp. 98-101 (1989)	
	D258	Baumgartner et al, “Differentiated Services: A New Approach for Quality of Service in the Internet,” International Conference on High Performance Networking, 255-273 (1998)	
	D259	Chapman et al., “Domain Name System (DNS),” 278-296 (1995)	
	D260	Davila et al., “Implementation of Virtual Private Networks at the Transport Layer,” M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D261	De Raadt et al., “Cryptography in OpenBSD,” 9 pages (1999)	
	D262	Eastlake, “Domain Name System Security Extensions,” Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	
	D263	Gunter et al., “An Architecture for Managing QoS-Enabled VRNs Over the Internet,” Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	21	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D264	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D265	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D266	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	D267	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	
	D268	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	D269	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D270	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D271	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D272	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D273	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	22	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages.	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages.	
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages.	
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	
	D299	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	
	D300	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D301	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D302	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D303	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D304	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D305	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D306	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D307	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	23	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D308	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D309	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D310	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D311	Tannenbaum, "Computer Networks," pages 202-219 (1996)	
	D312	Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D315	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D317	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D318	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D319	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D320	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D321	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D322	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D323	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D324	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D325	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D326	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent.	
	D327	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D328	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D329	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D330	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D331	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D332	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D333	Exhibit 19, RFC 2595 vs. Claims of the '211 Patent	
	D334	Exhibit 20, RFC 2595 vs. Claims of the '504 Patent	
	D335	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D336	Exhibit 22, iPASS vs. Claims of the '211 Patent	
	D337	Exhibit 23, iPASS vs. Claims of the '504 Patent	
	D338	Exhibit 24, "US '034" vs. Claims of the '135 Patent	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034") vs. Claims of the '211 Patent	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034") vs. Claims of the '504 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
				Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Filing Date*	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	24	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D341	Exhibit 27, US '287 vs. Claims of the '135 Patent	
	D342	Exhibit 28, US '287 vs. Claims of the '211 Patent	
	D343	Exhibit 29, US '287 vs. Claims of the '504 Patent	
	D344	Exhibit 30, Overview of Access VPNs vs. Claims of the '135 Patent	
	D345	Exhibit 31, Overview of Access VPNs vs. Claims of the '211 Patent	
	D346	Exhibit 32, Overview of Access VPNs vs. Claims of the '504 Patent	
	D347	Exhibit 34, RFC 1928 vs. Claims of the '135 Patent	
	D348	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D349	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D350	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D351	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D352	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D353	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D354	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D355	Exhibit 42,SecureConnect vs. Claims of the '504 Patent	
	D356	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D357	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D358	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D359	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D360	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D361	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D362	Exhibit 49, US '132 vs. Claims of the '135 Patent	
	D363	Exhibit 50, US '132 vs. Claims of the '211 Patent	
	D364	Exhibit 51, US '132 vs. Claims of the '504 Patent	
	D365	Exhibit 52, US '213 vs. Claims of the '135 Patent	
	D366	Exhibit 53, US '213 vs. Claims of the '211 Patent	
	D367	Exhibit 54, US '213 vs. Claims of the '504 Patent	
	D368	Exhibit 55, B&M VPNs vs. Claims of the '135 Patent	
	D369	Exhibit 56, B&M VPNs vs. Claims of the '211 Patent	
	D370	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D371	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D372	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D373	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D374	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D375	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D376	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D377	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D378	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	25	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D379	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D380	Exhibit 67, RFC 2486 vs. Claims of the '135 Patent	
	D381	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D382	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D383	Exhibit 70, Understanding IPSec vs. Claims of the '135 Patent	
	D384	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D385	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D386	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D387	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D388	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D389	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D390	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D391	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D392	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D393	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D394	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D395	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D396	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D397	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D398	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D399	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D400	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D401	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D402	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D403	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D404	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D405	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D406	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D407	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D408	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D409	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D410	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D411	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D412	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D413	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D414	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D415	Exhibit 102, NIKKEI vs. Claims of the '211 Patent	
	D416	Exhibit 103, NIKKEI vs. Claims of the '504 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 26	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D417	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D418	Exhibit 105, Omron vs. Claims of the '135 Patent	
	D419	Exhibit 106, Gauntlet System vs. Claims of the '135 Patent	
	D420	Exhibit 107, Gauntlet System vs. Claims of the '151 Patent	
	D421	Exhibit 108, Gauntlet System vs. Claims of the '180 Patent	
	D422	Exhibit 109, Gauntlet System vs. Claims of the '211 Patent	
	D423	Exhibit 110, Gauntlet System vs. Claims of the '504 Patent	
	D424	Exhibit 111, Gauntlet System vs. Claims of the '759 Patent	
	D425	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D426	Exhibit 113, IntraPort System vs. Claims of the '151 Patent	
	D427	Exhibit 114, IntraPort System vs. Claims of the '180 Patent	
	D428	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D429	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D430	Exhibit 117, IntraPort System vs. Claims of the '759 Patent	
	D431	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D432	Exhibit 119, Altiga VPN System vs. Claims of the '151 Patent	
	D433	Exhibit 120, Altiga VPN System vs. Claims of the '180 Patent	
	D434	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D435	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D436	Exhibit 123, Altiga VPN System vs. Claims of the '759 Patent	
	D437	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D438	Exhibit 125, Kiuchi vs. Claims of the '151 Patent	
	D439	Exhibit 126, Kiuchi vs. Claims of the '180 Patent	
	D440	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D441	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D442	Exhibit 129, Kiuchi vs. Claims of the '759 Patent	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '151 Patent	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '180 Patent	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D448	Exhibit 135, Overview vs. Claims of the '759 Patent	
	D449	Exhibit 136, RFC 2401 vs. Claims of the '759 Patent	
	D450	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO		**Complete if Known**	
		Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
(Use as many sheets as necessary)		Examiner Name	Dennis G. Bonshock
Sheet 27	of 52	Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D451	Exhibit 138, Schulzrinne vs. Claims of the '151 Patent	
	D452	Exhibit 139, Schulzrinne vs. Claims of the '180 Patent	
	D453	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D454	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D455	Exhibit 142, Schulzrinne vs. Claims of the '759 Patent	
	D456	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D457	Exhibit 144, Solana vs. Claims of the '151 Patent	
	D458	Exhibit 145, Solana vs. Claims of the '180 Patent	
	D459	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D460	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D461	Exhibit 148, Solana vs. Claims of the '759 Patent	
	D462	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D463	Exhibit 150, Atkinson vs. Claims of the '151 Patent	
	D464	Exhibit 151, Atkinson vs. Claims of the '180 Patent	
	D465	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D466	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D467	Exhibit 154, Atkinson vs. Claims of the '759 Patent	
	D468	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D469	Exhibit 156, Marino vs. Claims of the '151 Patent	
	D470	Exhibit 157, Marino vs. Claims of the '180 Patent	
	D471	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D472	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D473	Exhibit 160, Marino vs. Claims of the '759 Patent	
	D474	Exhibit 161, Aziz ('646) vs. Claims of the '759 Patent	
	D475	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D476	Exhibit 163, Wesinger vs. Claims of the '151 Patent	
	D477	Exhibit 164, Wesinger vs. Claims of the '180 Patent	
	D478	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D479	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D480	Exhibit 167, Wesinger vs. Claims of the '759 Patent	
	D481	Exhibit 168, Aziz ('234) vs. Claims of the '135 Patent	
	D482	Exhibit 169, Aziz ('234) vs. Claims of the '151 Patent	
	D483	Exhibit 170, Aziz ('234) vs. Claims of the '180 Patent	
	D484	Exhibit 171, Aziz ('234) vs. Claims of the '211 Patent	
	D485	Exhibit 172, Aziz ('234) vs. Claims of the '504 Patent	
	D486	Exhibit 173, Aziz ('234) vs. Claims of the '759 Patent	
	D487	Exhibit 174, Schneider vs. Claims of the '759 Patent	
	D488	Exhibit 175, Valencia vs. Claims of the '135 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	28	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D489	Exhibit 176, Valencia vs. Claims of the '151 Patent	
	D490	Exhibit 177, Valencia vs. Claims of the '180 Patent	
	D491	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D492	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867 vs. Claims of the '180 Patent	
	D494	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D495	Exhibit 182, Davison vs. Claims of the '151 Patent	
	D496	Exhibit 183, Davison vs. Claims of the '180 Patent	
	D497	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D498	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D499	Exhibit 186, Davison vs. Claims of the '759 Patent	
	D500	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D501	Exhibit 188, AutoSOCKS v2.1 vs. Claims of the '151 Patent	
	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide vs. Claims of the '180 Patent	
	D503	Exhibit 190, AutoSOCKS vs. Claims of the '759 Patent	
	D504	Exhibit 191, Aventail Connect 3.01/2.51 vs. Claims of the '135 Patent	
	D505	Exhibit 192, Aventail Connect v3.01/2.51 vs. Claims of the '151 Patent	
	D506	Exhibit 193, Aventail Connect 3.01/2.51 vs. Claims of the '180 Patent	
	D507	Exhibit 194, Aventail Connect 3.01/2.51 vs. Claims of the '759 Patent	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '135 Patent	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '151 Patent	
	D510	Exhibit 197, Aventail Connect 3.1/2.6 vs. Claims of the '180 Patent	
	D511	Exhibit 198, Aventail Connect 3.1/2.6 vs. Claims of the '759 Patent	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '151 Patent	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 Patent	
	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D517	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D518	Exhibit 205, Domain Name System (DNS) Security vs. Claims of the '504 Patent	
	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	29	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '135 Patent	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '151 Patent	
	D528	Exhibit 215, U.S. Patent No. 6,643,701 vs. Claims of the '135 Patent	
	D529	Exhibit 216, U.S. Patent No. 6,643,701 vs. Claims of the '151 Patent	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '151 Patent	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '135 Patent	
	D532	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D533	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '151 Patent	
	D535	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D536	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '151 Patent	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System vs. Claims of the '759 Patent	
	D546	Exhibit A: Copy of U.S. Patent No. 6,502,135	
	D547	Exhibit A: Copy of U.S. Patent No. 7,490,151	
	D548	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D549	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D550	Exhibit B-1: File History of U.S. Patent 6,502,135	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	***Complete if Known***
	Control Number | 95/001,949
	Filing Date | March 28, 2012
	First Named Inventor | Victor Larson
	Art Unit | 3992
	Examiner Name | Dennis G. Bonshock
Sheet | 30 | of | 52	*Attorney Docket Number* | 077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D551	Exhibit B-2: Reexamination Record No. 95/001,269	
	D552	Exhibit C1: Claim Chart – Aventail Connect v3.1 (Patent No. 6,502,135)	
	D553	Exhibit C2: Claim Chart Aventail Connect V3.01 (Patent No. 6,502,135)	
	D554	Exhibit C-1: Copy of U.S. Patent No. 7,010,604	
	D555	Exhibit C2: Claim Chart Aventail Autosocks (Patent No. 7,490,151)	
	D556	Exhibit C1: Claim Chart Aventail Connect v3.01 (Patent No. 7,490,151)	
	D557	Exhibit C-2: Provisional Application 60/106,261	
	D558	Exhibit C3: Claim Chart Aventail AutoSOCKS (Patent No. 6,502,135)	
	D559	Exhibit C3: Claim Chart BinGO (Patent No. 7,490,151)	
	D560	Exhibit C-3: Provisional Application 60/137,704	
	D561	Exhibit C4: Claim Chart Wang (Patent No. 6,502,135)	
	D562	Exhibit C4: Claim Chart Beser (Patent No. 7,490,151)	
	D563	Exhibit C5: Claim Chart Beser (Patent No. 6,502,135)	
	D564	Exhibit C5: Claim Chart Wang (Patent No. 7,490,151)	
	D565	Exhibit C6: Claim Chart BinGO (Patent No. 6,502,135)	
	D566	Exhibit D: Memorandum Opinion in *VirnetX v. Microsoft.*	
	D567	Exhibit D-1: Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HPPT-Based Network on the Internet," Published in the Proceedings of SNDSS 1996.	
	D568	Exhibit D-10: D.E. Denning and G.M. Sacco, "Time-stamps in Key Distribution Protocols," Communications of the ACM, Vol. 24, N.8, pp. 533-536. August 1981.	
	D569	Exhibit D-11: C.I. Dalton and J.F. Griffin, "Applying Military Grade Security to the Internet," Proceedings of the 8th Joint European Networking Conference (JENC 8), (May 12-15 1997).	
	D570	Exhibit D-12: Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based protocols Secure against Dictionary Attacks," 1992 IEEE Symposium on Security and Privacy (1992).	
	D571	Exhibit D-2: Copy of U.S. Pat. No. 5,898,830	
	D572	Exhibit D-3: Eduardo Solana and Jürgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains," Security Protocols Workshop 1997, pp. 37-51.	
	D573	Exhibit D-4: Copy of U.S. Pat. No. 6,119,234	
	D574	Exhibit D-5: Jeff Sedayao, "Mosaic Will Kill My Network!' – Studying Network Traffic Patterns of Mosaic Use," in Electron. Proc. 2nd World Wide Web Conf. '94: Mosaic and the Web, Chicago, IL, Oct. 1994.	
	D575	Exhibit D-6: M. Luby Juels and R. Ostrovsky, "Security of Blind Digital Signatures," Crypto '97, LNCS 1294, pages 150-164, Springer-Verlag, Berlin, 1997.	
	D576	Exhibit D-8: David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).	
	D577	Exhibit D-9: Copy of U.S. Pat. No. 7,764,231	
	D578	Exhibit E-1: Claim Charts Applying Kiuchi and Other References to Claims of the '135 Patent.	
	D579	Exhibit E1: Declaration of Chris Hopen (Patent No. 6,502,135)	
	D580	Exhibit E1: Declaration of Chris Hopen (Patent No. 7,490,151)	
	D581	Exhibit E-2: Claim Charts Applying Wesinger and Other References to Claims of the '135 Patent.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	31	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D582	Exhibit E2: Declaration of Michael Fratto (Patent No. 6,502,135)	
	D583	Exhibit E2: Declaration of Michael Fratto (Patent No. 7,490,151)	
	D584	Exhibit E-3: Claim Charts Applying Solana and Other References to Claims of the '135 Patent.	
	D585	Exhibit E3: Declaration of James Chester (Patent No. 6,502,135)	
	D586	Exhibit E3: Declaration of James Chester (Patent No. 7,490,151)	
	D587	Exhibit E-4: Claim Charts Applying Aziz and Other References to Claims of the '135 Patent.	
	D588	Exhibit X1: Aventail Connect Administrator's Guide v3.1/v2.6., PP 1-20 (1996-1999)	
	D589	Exhibit X10: Copy of U.S. Patent No. 4,885,778	
	D590	Exhibit X11: Copy of U.S. Patent No. 6,615,357	
	D591	Exhibit X2: Aventail Connect Administrator's Guide v3.01/v2.51., PP 1-116 (1996-1999)	
	D592	Exhibit X3: Aventail AutoSOCKS Administration & User's Guide v2.1., PP 1-70 (1996-1999)	
	D593	Exhibit X4: Reed et al., "Proxies for Anonymous Routine," 12th Annual Computer Security Applications Conference, San Diego, CA, December -9-13, pp 1-10 (1996).	
	D594	Exhibit X5: Wang, The Broadband Forum Technical Report, "TR-025 – Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL," Issue 1.0; pp. 1-24 , v1.0 (1999).	
	D595	Exhibit X6: Copy of U.S. Patent No. 6,496,867	
	D596	Exhibit X7: BinGO! User's Guide Incorporating by Reference BinGO! Extended Feature Reference.	
	D597	Exhibit X7: Kent et al., "Security Architecture for the Internet Protocol, " Network Working Group Request for Comments (RFC) 2401, pp 1-70 (1998).	
	D598	Exhibit X8: Copy of U.S. Patent No. 6,182,141	
	D599	Exhibit X9: BinGO! User's Guide v1.6 (1999).	
	D600	Exhibit Y1: Aventail Extranet Server 3.0 Administrator's Guide.	
	D601	Exhibit Y10: Hanks, S., et al., RFC1701, "Generic Routing Encapsulation (GRE)," 1994, Is Accessbile at http://www.ietf.org/rfc/rfc1701.txt.	
	D602	Exhibit Y10: Socolofsky, T. et al., RFC 1180, "A TCP/IP Tutorial," January 1991.	
	D603	Exhibit Y11: Simpson, W., editor, RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994.	
	D604	Exhibit Y11: Simpson, W., RFC1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," 1996, http://www.ietf.org/rdc/rfc1994.txt.	
	D605	Exhibit Y12: Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996.	
	D606	Exhibit Y12: Perkins, D., RFC1171, "The Point-To-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-To-Point Links," 1990, Is Accessible at http://www.ietf.org/rfc/rfc1171.txt.	
	D607	Exhibit Y13: Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September, 1998.	
	D608	Exhibit Y14: Townsley, W.M., et al., RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999.	
	D609	Exhibit Y15: Pall, G.S., RFC 2118, "Microsoft Point-To-Point Encryption (MPPE) Protocol," March 1997.	
	D610	Exhibit Y16: Gross, G., et al., RFC 2364, "PPP Over AAL5," July 1998.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	***Complete if Known***	
	Control Number	95/001,949
	Filing Date	March 28, 2012
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Dennis G. Bonshock
Sheet 32 of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D611	Exhibit Y17: Srisuresh, P., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999.	
	D612	Exhibit Y18: Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993.	
	D613	Exhibit Y2: Goldschlag et al., "Hiding Routing Information" (1996).	
	D614	Exhibit Y3: Copy of U.S. Patent No. 5,950,519	
	D615	Exhibit Y4: Ferguson, P. and Huston, G., "What Is a VPN", The Internet Protocol Journal, Vol 1., No. 1 (June 1998 ("Ferguson").	
	D616	Exhibit Y5: Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC1034").	
	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodburn, R.A., et al., RFC1241, "A Scheme for an Internet Encapsulation Protocol: Version 1," 1991.	
	D620	Exhibit Y9: Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996.	
	D621	Exhibit Y9: Simpson, W., RFC1853, "IP in IP Tunneling," 1995, Is Accessible at http://ww.ietf.org/rfc/rfc1583.txt.	
	D622	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 6,502,135)	
	D623	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 7,490,151)	
	D624	Request for Inter Partes Reexamination (Patent No. 6,502,135)	
	D625	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 6,502,135)	
	D626	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 7,490,151)	
	D627	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D628	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D629	Transmittal Letter (Patent No. 6,502,135)	
	D630	Transmittal Letter (Patent No. 7,490,151)	
	D631	Joint Claim Construction and Prehearing Statement	
	D632	Exhibit A: Agreed Upon Terms; P.R. 4-3 Joint Claims Construction and Prehearing Statement	
	D633	Exhibit B: Disputed Claim Terms; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D634	Exhibit C; VirnetX's Proposed Construction of Claim Terms and Supporting Evidence	
	D635	Exhibit D; Defendants' Intrinsic and Extrinsic Support; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D636	U.S. Patent 6,839,759	
	D637	Exhibit B-4; VirnetX, Inc. v. Microsoft Corp., Case No. 6:07-cv-80, Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759 (E.D. Tex. Dec. 18, 2009)	
	D638	Exhibit D-2; Kent et al., "Security Architecture for the Internet Protocol," Internet Engineering Task Force, Internet Draft, (Feb. 1998)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	33	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D639	Exhibit D-3; Aziz et al., U.S. Patent 5,548,646 to Aziz et al., "System for Signatureless Transmission and Reception of Data Packets Between Computer Networks," Filed Sept. 15, 1994 and issued Aug. 20, 1996	
	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Internet Protocol," DARPA Internet Program Specification RFC 791 (Sept. 1981)	
	D644	Exhibit D-14; Caronni et al., "SKIP – Securing the Internet," 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '96) (June 19-21, 1996)	
	D645	Exhibit D-15; Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP), " IPSEC Work Group Draft (July 26, 1997)	
	D646	Exhibit E-1; Claim Charts Applying Kiuchi as a Primary Reference to the '759 Patent.	
	D647	Exhibit E-2; Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D648	Exhibit E-3; Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D649	Exhibit E-4; Claim Charts Applying Kent in view of Caronni as a Primary Combination of References to the '759 Patent	
	D650	Exhibit D-5; Edwards et al., "High Security Web Servers and Gateways," Computer Networks and ISDN System 29, pages 927-938 (Sept. 1997)	
	D651	Exhibit D-10; Lee et al., "Hypertext Transfer Protocol – HTTP/1.0," RFC 1945 (May 1996)	
	D652	Exhibit E-3; Claim Charts Applying Blum to Claims of the '151 Patent	
	D653	Exhibit B-1, File History of U.S. Patent 7,490,151	
	D654	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D655	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D656	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D657	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D658	VirnetX Inc., V. Mitel Networks Corp.; Defendants' Joint Invalidity Contentions	
	D659	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D660	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D661	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D662	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D663	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D664	Exhibit 42, SecureConnect vs. Claims of the '504 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	34	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D665	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D666	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D667	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D668	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D669	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D670	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D671	Exhibit 49, Chuah vs. Claims of the '135 Patent	
	D672	Exhibit 50, Chuah vs. Claims of the '211 Patent	
	D673	Exhibit 51, Chuah vs. Claims of the '504 Patent	
	D674	Exhibit 52, U.S. '648 vs. Claims of the '135 Patent	
	D675	Exhibit 53, U.S. '648 vs. Claims of the '211 Patent	
	D676	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D677	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D678	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D679	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D680	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D681	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D682	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D683	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D684	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D685	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D686	Exhibit 67, US '072 vs. Claims of the '135 Patent	
	D687	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D688	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D689	Exhibit 70 Understanding IPSec vs. Claims of the '135 Patent	
	D690	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D691	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D692	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D693	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D694	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D695	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D696	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D697	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D698	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D699	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D700	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D701	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D702	Exhibit 83, US '261 vs. Claims of the '211 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	35	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D703	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D704	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D705	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D706	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D707	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D708	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D709	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D710	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D711	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D712	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D713	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D714	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D715	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D716	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D717	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D718	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D719	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D720	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D721	Exhibit 102, Nikkei vs. Claims of the '211 Patent	
	D722	Exhibit 103, Nikkei vs. Claims of the '504 Patent	
	D723	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D724	Exhibit 106-A, Gauntlet System vs. Claims of the '135 Patent	
	D725	Exhibit 109-A, Gauntlet System vs. Claims of the '211 Patent	
	D726	Exhibit 110-A, Gauntlet System vs. Claims of the '504 Patent	
	D727	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D728	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D729	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D730	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D731	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D732	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D733	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D734	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D735	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D736	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D737	Exhibit 137, Schulzrinne vs. Claims of the '135 (Final) Patent	
	D738	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D739	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D740	Exhibit 143, Solana vs. Claims of the '135 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	36	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D741	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D742	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D743	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D744	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D745	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D746	Exhibit 168, Aziz vs. Claims of the '135 Patent	
	D747	Exhibit 171, U.S. '234 vs. Claims of the '211 Patent	
	D748	Exhibit 172, Aziz vs. Claims of the '504 Patent	
	D749	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D750	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D751	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D752	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D753	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D754	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP' vs. Claims of the '135 Patent	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401' vs. Claims of the '135 Patent	
	D763	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D764	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D765	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D766	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D768	Exhibit 228, U.S. 588 vs. Claims of the '211 Patent (Final)	
	D769	Exhibit 229, U.S. 588 vs. Claims of the '504 Patent (Final)	
	D770	Exhibit 230, Microsoft VPN vs. Claims of the '135 Patent (Final)	
	D771	Exhibit 231, Microsoft VPN vs. Claims of the '211 Patent (Final)	
	D772	Exhibit XX, Microsoft VPN vs. Claims of the '504 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
				Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Filing Date*	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	37	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D773	Exhibit Cisco-1, Cisco's Prior Art System vs. Claims of the '135 Patent	
	D774	Exhibit Cisco-4, Cisco's Prior Art System vs. Claims of the '211 Patent	
	D775	Exhibit Cisco-5, Cisco's Prior Art System vs. Claims of the '504 Patent	
	D776	Exhibit 225, US '037 vs. Claims of the '135 Patent	
	D777	Exhibit 226, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D778	Exhibit 227, US '393 vs. Claims of the '135 Patent	
	D779	Exhibit 233, The Miller Application vs. Claim 13 of the '135 Patent	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '504 Patent	
	D781	Exhibit 235, Microsoft VPN vs. Claims of the '504 Patent	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '211 Patent	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '504 Patent	
	D784	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D785	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D786	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D787	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D788	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D789	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D790	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D791	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D792	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D793	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent	
	D794	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D795	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D796	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D797	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D798	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D799	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D800	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D801	Exhibit 22, iPass vs. Claims of the '211 Patent	
	D802	Exhibit 23, iPass vs. Claims of the '504 Patent	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ("034 Patent") vs. Claims of the '135 Patent	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ("034 Patent") vs. Claims of the '211 Patent	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ("034 Patent") vs. Claims of the '504 Patent	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the '135 Patent	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the '211 Patent	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the '504 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**
				Control Number 95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Filing Date* March 28, 2012
				First Named Inventor Victor Larson
				Art Unit 3992
(Use as many sheets as necessary)				*Examiner Name* Dennis G. Bonshock
Sheet	38	of	52	*Attorney Docket Number* 077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D809	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D810	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D811	Exhibit 106, Gaunlet System and Gaunlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gaunlet System and Gaunlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gaunlet System vs. Claims of the '504 Patent	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D817	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D818	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D819	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D820	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D821	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D822	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D823	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect") vs. Claims of the '135 Patent	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '135 Patent	
	D826	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D827	Exhibit 205, Domain Name System (DNS) Security ("DNS Security") vs. Claims of the '504 Patent	
	D828	Exhibit 210, Lendenmann vs. Claims of the '211 Patent	
	D829	Exhibit 211, Lendenmann vs. Claims of the '504 Patent	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D831	Exhibit 215, Aziz vs. Claims of the '135 Patent	
	D832	Cisco '180, Efiling Acknowledgment	
	D833	Exhibit A, U.S. Patent 7,188,180	
	D834	Exhibit B1, File History of U.S. Patent 7,188,180	
	D835	Exhibit B2, File History of U.S. Patent Application No. 09/588,209	
	D836	Exhibit B3, File History of Reexamination Control No. 95/001,270, Reexamination of U.S. 7,188,180 requested by Microsoft Corp	
	D837	Exhibit D1, "Lendenmann": Rolf Lendenman, Understanding OSF DCE 1.1 For AIX and OS/2, IBM International Technical Support Organization (Oct. 1995).	
	D838	Exhibit D5, "Schneier": Bruce Schneier, Applied Cryptography (1996)	
	D839	Exhibit D6, RFC 793; Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Specification RFC 793 (Sept. 1981)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	39	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	
	D841	Exhibit D8, "Rosenberry"; Ward Rosenberry, David Kenney, and Gerry Fisher, Understanding DCE (1993)	
	D842	Exhibit D9, Masys; Daniel R. Masys & Dixie B. Baker, "Protecting Clinical Data on Web Client Computers: The PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, Florida (Nov. 7-11, 1998)	
	D843	Exhibit E1, Claim Charts Applying Lendenmann as a Primary Reference to the '180 Patent.	
	D844	Exhibit E2, Claim Charts Applying Kiuchi as a Primary Reference to the '180 Patent	
	D845	Exhibit E3, Claim Charts Applying Solana as a Primary Reference to the '180 Patent	
	D846	Exhibit E4, Claim Charts Applying Schimpf and Rosenberry as a Primary Reference to the '180 Patent	
	D847	Request for Inter Partes Reexamination of Patent No. 7,188,180	
	D848	Modified PTO Form 1449	
	D849	Request for Inter Partes Reexamination Transmittal Form No. 7,188,180	
	D850	Exhibit A; U.S. Patent 7,921,211 with Terminal Disclaimer	
	D851	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,921,211)	
	D852	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D853	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D854	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser)	
	D855	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D856	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D857	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D858	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D859	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D860	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D861	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D862	Exhibit X1, Solana, E. et al. "Flexible Internet Secure Transactions Based on Collaborative Domains"	
	D863	Exhibit X2, U.S. Patent 6,557,037	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**	
				Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Filing Date*	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	40	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D864	Exhibit X4, Atkinson, R., IETF RFC 2230, "Key Exchange Delegation Record for the DNS" (November 1997)	
	D865	Exhibit X6, Kent, et al., IETF RFC 2401, "Security Architecture for the Internet Protocol" (November 1998) Is Accessible at: http://www.ietf.org/rfc/rfc2401.txt	
	D866	Exhibit X7, Eastlake, D. et al., IETF RFC 2065, "Domain Name System Security Extensions" (January 1997) Is Accessible at: http://www.ietf.org/rfc/rfc2065.txt	
	D867	Exhibit X9, Guttman, E. et al., IETF RFC 2504, "Users' Security Handbook" (February 1999) Is Accessible At: http://www.ietf.org/rfc/rfc2504.txt	
	D868	Exhibit Y3, Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989 ("RFC1123").	
	D869	Exhibit Y4, Atkinson, R., RFC 1825, "Security Architecture for the Internet Protocol (August 1995) Is Accessible At: http://www.ietf.org/rfc/rfc1825.txt	
	D870	Exhibit Y5, Housley, R. et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (January 1999) Is accessible At: http://www.ietf.org/rfc/rfc2459.txt	
	D871	Exhibit A, U.S. Patent 7,418,504	
	D872	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,418,504)	
	D873	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D874	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in view of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D875	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D876	Exhibit C4, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D877	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed, and Beser	
	D878	Exhibit C6, Claim Chart – USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D879	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D880	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D881	Exhibit D1, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act. 6:2010cv00417 (E.D. Tex)	
	D882	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. against Apple Inc. Based on the 7,418,504	
	D883	Exhibit X5, Eastlake, D., et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)" (March 1999)	
	D884	Exhibit X6, Kent, S. IETF RFC 2401, "Security Architecture for the Internet Protocol, (November1998) http://www.ietf.org/rfc/rfc2401.txt	
	D885	Exhibit X8, Postel, J. et al., IETF RFC 920, "Domain Requirements" (October 1984) Is Accessible at http://www.ietf.org/rfc/rfc920.txt	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	41	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D886	Exhibit X10, Reed, M. et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996.	
	D887	Request for Inter Partes Reexamination Transmittal form	
	D888	Transmittal Letter	
	D889	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D890	Exhibit D-7, "Thomas": Brian Thomas, "Recipe for E-Commerce, IEEE Internet Computing, (Nov.-Dec. 1997)	
	D891	Exhibit D-9, "Kent II": Stephen Kent & Randall Atkinson, "IP Encapsulating Security Payload (ESP)," Internet Engineering Task Force, Internet Draft (Feb. 1998)	
	D892	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser (Came from Inval. Cisco dtd 11/18/11)	
	D893	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D894	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D895	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D896	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D897	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D898	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D899	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D900	211 Request for Inter Partes Reexamination	
	D901	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D902	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D903	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D904	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D905	Exhibit C6, USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D906	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D907	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D908	504 Request for Inter Partes Reexamination	
	D909	Defendants' Supplemental Joint Invalidity Contentions	
	D910	Exhibit 226, Securing Web Access with DCE vs. Claims of the '135 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	42	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D911	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D918	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D921	Exhibit 237, U.S. '648 vs. Claims of the '135 Patent	
	D922	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D923	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D924	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D925	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D926	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D927	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D928	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D929	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D930	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D931	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D932	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D933	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D934	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D936	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D937	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D938	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	D939	Exhibit A, Aventail Press Release, May 2, 1997	
	D940	Exhibit B, InfoWorld, "Aventail Delivers Highly Secure, Flexible VPN Solution," InfoWorld, page 64D, (1997)	
	D941	Exhibit C, Aventail AutoSOCKS v2.1 Administrator's Guide	
	D942	Exhibit D, Aventail Press Release, October 12, 1998	
	D943	Exhibit G, Aventail Press Release, May 26, 1999	
	D944	Exhibit H, Aventail Press Release, August 9, 1999	
	D945	Exhibit J, "Aventail ExtraNet Center 3.1: Security with Solid Management, Network Computing, June 28, 1999	
	D946	Petition in Opposition to Patent Owner's Petition to Vacate Inter Partes ReExamination Determination on Certain Prior Art	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	43	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D947	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D948	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under U.S.C. § 311	
	D949	Exhibit C1, Claim Chart Aventail Connect v3.1	
	D950	Exhibit C2, Claim Chart Aventail Connect v3.01	
	D951	Exhibit C3, Claim Chart Aventail AutoSOCKS	
	D952	Exhibit C4, Claim Chart Wang	
	D953	Exhibit C5, Claim Chart Beser	
	D954	Exhibit C6, Claim Chart BINGO	
	D955	Exhibit X6, U.S. Patent 6,496,867	
	D956	Exhibit X10, U.S. Patent 4,885,778	
	D957	Exhibit X11, U.S. Patent 6,615,357	
	D958	Exhibit Y3, U.S. Patent 5,950,519	
	D959	Request for Inter Partes Reexamination Transmittal Form	
	D960	Transmittal Letter	
	D961	Exhibit D, v3.1 Administrator's Guide	
	D962	Exhibit E-1, Claim Charts Applying Kiuchi to Various Claims of the '135 Patent	
	D963	Exhibit E-2, Claim Charts Applying Wesinger to Various Claims of the '135 Patent	
	D964	Exhibit E-3, Claim Charts Applying Solana to Various Claims of the '135 Patent	
	D965	Exhibit E-4, Claim Charts Applying Aziz to Various Claims of the '135 Patent	
	D966	Request for Inter Partes Reexamination Transmittal Form	
	D967	Request for Inter Partes Reexamination	
	D968	PTO Form 1449	
	D969	Exhibit C1, Claim Chart Aventail Connect v3.01	
	D970	Exhibit C2, Claim Chart Aventail AutoSOCKS	
	D971	Exhibit C3, Claim Chart BINGO	
	D972	Exhibit C4, Claim Chart Beser	
	D973	Exhibit C5, Claim Chart Wang	
	D974	Transmittal Letter	
	D975	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D976	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D977	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D978	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D979	Exhibit E-3, Claim Charts Applying Blum to Claims of the '151 Patent	
	D980	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D981	Exhibit E-5, Claim Charts Applying Kiuchi and Edwards, and Kiuchi, Edwards, and Martin to Claims of the '151 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
				Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Filing Date*	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	44	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D982	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D983	Exhibit A, U.S. Patent 6,839,759	
	D984	Exhibit C-1, U.S. Patent 6,502,135	
	D985	Exhibit E-1, Claim Charts Applying Kiuchi, as Primary Reference to the '759 Patent	
	D986	Exhibit E-2, Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D987	Exhibit E-3, Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D988	Exhibit E-4, Claim Charts Applying Kent in View of Caronni as a Primary Combination of References to the '759 Patent	
	D989	Request for Inter Partes Reexamination Transmittal Form	
	D990	Request for Inter Partes Reexamination	
	D991	PTO Form 1449	
	D992	Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D993	Request for Inter Partes Reexamination	
	D994	Request for Inter Partes Reexamination Transmittal Form	
	D995	Request for Inter Partes Reexamination	
	D996	Request for Inter Partes Reexamination Transmittal Form	
	D997	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D998	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D999	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D1000	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D1001	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D1002	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D1003	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1004	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1005	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D1006	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D1007	Exhibit B1, File History of U.S. Patent 7,418,504	
	D1008	Exhibit B2, File History of U.S. Patent Application No. 09/558,210	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

				Complete if Known	
IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Dennis G. Bonshock
Sheet	45	of	52	Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1009	Exhibit D-10, Gaspoz et al., "VPN on DCE: From Reference Configuration to Implementation," Bringing Telecommunication Services to the People – IS&N '95, Third International Conference on Intelligence in Broadband Services and Networks, October 1995 Proceedings, Lecture Notes in Computer Science, Vol. 998 (Springer, 1995)	
	D1010	Exhibit D-11, Copy of U.S. Patent No. 6,269,099	
	D1011	Exhibit D-11, Copy of U.S. Patent No. 6,560,634	
	D1012	Exhibit D-13, Pallen, "The World Wide Web," British Medical Journal, Vol. 311 at 1554 (Dec. 1995)	
	D1013	Exhibit D-14, Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21:120-126 (Feb. 1978)	
	D1014	Exhibit D-15, Copy of U.S. Patent No. 4,952,930	
	D1015	Exhibit D-17, Pfaffenberger, Netscape Navigator 3.0: Surfing the Web and Exploring the Internet, Academic Press (1996)	
	D1016	Exhibit D-18, Gittler et al., "The DCE Security Service," Hewlett-Packard Journal, pages 41-48 (Dec. 1995)	
	D1017	Exhibit D-6, Copy of U.S. Patent No. 5,689,641	
	D1018	Exhibit D-9, Lawton, "New Top-Level Domains Promise Descriptive Names," Sunworld Online, 1996	
	D1019	Exhibit E-1, Copy of Catalog Listing by IBM for RS/6000 Redbooks Collection which includes a Link to the *Lendenmann* reference. The link to the *Lendenmann* reference was archived at archive.org on December 7, 1998 and retrieved by the Wayback Machine	
	D1020	Exhibit E-10, copy of an Archived Version of the Lawton reference archived at archive.org on February 19, 1999 and retrieved by the Wayback Machine	
	D1021	Exhibit E-11, Abstracts of the Proceedings of the Symposium on Network and Distributed System Security, 1996, Archived at archive.org on April 10, 1997, and retrieved by the Wayback Machine	
	D1022	Exhibit E-12, 1996 Symposium on Network and Distributed System Security, Website Archived by archive.org (Apr. 10, 1997), Retrieved by the Wayback Machine at http://web.archive.org/web/19970410114853/http://computer.org/cspress/catalog/proc9.htm.	
	D1023	Exhibit E-13, Copy of Search Results for ISBN 0-12-553153-2 (Pfaffenberger) from www.isbnsearch.org	
	D1024	Exhibit F-1, Claim Charts applying Lendenmann as a Primary Reference to the '504 Patent.	
	D1025	Exhibit F-2, Claim Charts applying Aziz as a Primary Reference to the '504 Patent	
	D1026	Exhibit F-3, Claim Charts applying Kiuchi and Pfaffenberger as Primary References to the '504 Patent	
	D1027	Exhibit E-2, First Page of U.S. Patent No. 5,913,217 published June 15, 1999 and citing a portion of the Lendenmann reference as a prior art reference	
	D1028	Exhibit E-3, Request for Comments 2026, "The Internet Standards Process – Revision 3," October 1996	
	D1029	Exhibit E-4, First Page of U.S. 5,463,735, published October 31, 1995 and citing RFC 793 as a prior art Reference	
	D1030	Exhibit E-5, Copy of catalog listing from Boston University Digital Common Website, listing the Martin reference with an issue date of February 21, 1998	
	D1031	Exhibit E-6, Copy of Technical Reports Archive Listing from Boston University Computer Science Department which includes a link to the Martin paper. The link to the Martin paper was archived at archive.org on January 22, 1998 and Retrieved by the Wayback Machine	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	46	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1032	Exhibit E-7, Boston University Computer Science Department Technical Reports Instructions, available at: http://www.cs.bu.edu/techreports/INSTRUCTIONS	
	D1033	Exhibit E-8, U. Möller, "Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe," Diplomarbeit, Universität Hamburg (July 16, 1999), citing to Martin at page 77.	
	D1034	Exhibit E-9, First page of U.S. 5,737,423, published April 7, 1998 and citing Schneier as Prior Art Reference	
	D1035	Request for Inter Partes ReExamination; U.S. Patent 7,418,504	
	D1036	Request for Inter Partes ReExamination Transmittal Form; U.S. Patent 7,418,504	
	D1037	PTO Form 1449	
	D1038	Exhibit C1, Claim Chart – USP 7,921,211 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1039	Exhibit C2, Claim Chart – USP 7,921,211 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1040	Exhibit C3, Claim Chart – USP 7,921,211 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1041	Exhibit C4, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2230 and further in conjunction with RFC 920, Reed and Beser	
	D1042	Exhibit C5, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1043	Exhibit C6, Claim Chart – USP 7,921,211relative to Beser, Alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1044	Exhibit C7, Claim Chart – USP 7,921,211 relative to RFC 2230, alone and in conjunction with RFC 2401, Reed, and Beser	
	D1045	Exhibit C8, Claim Chart – USP 7,921,211 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1046	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1047	Exhibit C1, Claim Chart – USP 7,418,504 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1048	Exhibit C2, Claim Chart – USP 7,418,504 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1049	Exhibit C3, Claim Chart – USP 7,418,504 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1050	Exhibit C5, Claim Chart – USP 7,418,504 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1051	Exhibit C6, USP 7,418,504 relative to Beser, alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1052	Exhibit C7, Claim Chart – USP 7,418,504 relative to RFC 2230, alone and in conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1053	Exhibit C8, Claim Chart – USP 7,418,504 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1054	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1055	Exhibit 226, Securing Web Access with DCE vs. Claims of the '135 Patent	
	D1056	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	47	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D1063	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D1064	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D1065	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D1066	Exhibit 237, U.S. '072 vs. Claims of the '135 Patent	
	D1067	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D1068	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D1069	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D1070	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D1071	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D1072	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D1073	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D1074	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D1075	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D1076	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D1077	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D1078	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D1079	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D1081	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D1083	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	D1084	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1087	Exhibit B1, File History of U.S. Patent 7,921,211	
	D1088	Exhibit B2, File History of U.S. Patent Application No. 10/714,849	
	D1089	Exhibit B4, *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009)	
	D1090	Exhibit D15, U.S. Patent 4,952,930	
	D1091	Exhibit F1, Claim Charts Applying Lendenmann as a Primary Reference to the '211 Patent	
	D1092	Exhibit F2, Claim Charts Applying Aziz as a Primary Reference to the '211 Patent	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 48	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1093	Exhibit F3, Claim Charts Applying Kiuchi and Pfaffenberger as Primary References to the '211 Patent	
	D1094	Exhibit 2, Letter and attachment from Ramzi Khazen, Counsel for VirnetX, to Dmitriy Kheyfits, Counsel for Cisco Systems (June 23, 2011)	
	D1095	Exhibit P, Malkin, "Dial-In Virtual Private Networks Using Layer 3 Tunneling"	
	D1096	Exhibit Q, Ortiz, "Virtual Private Networks: Leveraging the Internet"	
	D1097	Exhibit R, Keromytix, "Creating Efficient Fail-Stop Cryptographic Protocols"	
	D1098	Transcript of Markman Hearing Dated January 5, 2012	
	D1099	Declaration of John P. J. Kelly, Ph.D	
	D1100	Defendants' Responsive Claim Construction Brief; Exhibits A–P and 1-7	
	D1101	Joint Claim Construction and Prehearing Statement Dated 11/08/11	
	D1102	Exhibit A: Agreed Upon Terms Dated 11/08/11	
	D1103	Exhibit B: Disputed Claim Terms Dated 11/08/11	
	D1104	Exhibit C: VirnetX's Proposed Construction of Claim Terms and Supporting Evidence Dated 11/08/11	
	D1105	Exhibit D: Defendant's Intrinsic and Extrinsic Support Dated 11/08/11	
	D1106	Declaration of Austin Curry in Support of VirnetX Inc.'s Opening Claim Construction Brief	
	D1107	Declaration of Mark T. Jones Opening Claims Construction Brief	
	D1108	VirnetX Opening Claim Construction Brief	
	D1109	VirnetX Reply Claim Construction Brief	
	D1110	European Search Report from corresponding EP Application Number 11005789 (Our Ref.: 077580-0142)	
	D1111	European Search Report from corresponding EP Application Number 11005792 (Our Ref.: 077580-0143)	
	D1112	ITU-T Recommendation H.323, "Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System," International Telecommunications Union, pages 1-128, February 1998	
	D1113	ITU-T Recommendation H.225.0, "Infrastructure of Audiovisual Services – Transmission Multiplexing and Synchronization. Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication systems," International Telecommunication Union, pages 1-155, February 1998	
	D1114	ITU-T Recommendation H.235, "Infrastructure of Audiovisual Services – Systems Aspects. Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals," International Telecommunication Union, pages 1-39, February 1998	
	D1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	D1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	D1117	Transmittal Letters (Patent No.8,051,181)	
	D1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	
	D1119	Transcript of Hopen Deposition dated April 11, 2012 (57 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	49	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1120	Claim Construction Memorandum Opinion and Order in Case No. 6:10-CV-417 (31 pages)	
	D1121	Declaration of Angelos D. Keromytic, Ph.D. in Control No. 95/001,682 (98 pages)	
	D1122	Declaration of Dr. Robert Dunham Short III in Control Nos. 95/001,679; 95/001,682 (6 pages)	
	D1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.) (2 pages)	
	D1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. in Control No. 95/001,269 (9 pages)	
	D1125	Exhibit A-4, Redacted Deposition of Chris Hopen from VirnetX, Inc. v. Cisco Systems, Inc., No. 6:07-CV 417 (E.D. Tex. April 11, 2012 (5 pages)	
	D1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999 (23 pages)	
	D1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects (95 pages)	
	D1128	Exhibit B-3, Maryann Lawlor, Transient Partnerships Stretch Security Policy Management, Signal Magazine (Sept. 2001) http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes (5 pages)	
	D1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html. (5 pages)	
	D1130	Time Greene, CEO's Chew the VPN Fat, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch (6 pages)	
	D1131	Peter Alexander Invalidity Report in Case No. 6:10-cv-000417 (220 pages)	
	D1132	Defendants' Second Supplemental Joint Invalidity Contentions in Case No. 6:10-cv-0417 (3 pages)	
	D1133	Exhibit 118A, Altiga VPN System vs. Claims of the '135 Patent (251 pages)	
	D1134	Exhibit 119A, Altiga VPN System vs. Claims of the '151 Patent (73 pages)	
	D1135	Exhibit 120A, Altiga VPN System vs. Claims of the '180 Patent (78 pages)	
	D1136	Exhibit 121A, Altiga VPN System vs. Claims of the '211 Patent (95 pages)	
	D1137	Exhibit 122A, Altiga VPN System vs. Claims of the '504 Patent (95 pages)	
	D1138	Exhibit 123A, Altiga VPN System vs. Claims of the '759 Patent (123 pages)	
	D1139	Exhibit 12A, SSL 3.0 vs. Claims of the '135 Patent (25 pages)	
	D1140	Exhibit 13A, SSL 3.0 vs. Claims of the '504 Patent (33 pages)	
	D1141	Exhibit 14A, SSL 3.0 vs. Claims of the '211 Patent (33 pages)	
	D1142	Exhibit 228A, Understanding OSF DCE 1. for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '135 Patent (21 pages)	
	D1143	Exhibit 229A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '151 Patent (15 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	50	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1144	Exhibit 230A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '180 Patent (25 pages)	
	D1145	Exhibit 231A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '211 Patent[2]	
	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '504 Patent (44 pages)	
	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '759 Patent (28 pages)	
	D1148	Exhibit 255, Schulzrinne vs. Claims of the '135 Patent (28 pages)	
	D1149	Exhibit 256, Schulzrinne vs. Claims of the '504 Patent (122 pages)	
	D1150	Exhibit 257, Schulzrinne vs. Claims of the '211 Patent (122 pages)	
	D1151	Exhibit 258, Schulzrinne vs. Claims of the '151 Patent (49 pages)	
	D1152	Exhibit 259, Schulzrinne vs. Claims of the '180 Patent (41 pages)	
	D1153	Exhibit 260, Schulzrinne vs. Claims of the '759 Patent (74 Pages)	
	D1154	Exhibit 261, SSL 3.0 vs. Claims of the '151 Patent (14 pages)	
	D1155	Exhibit 262, SSL 3.0 vs. Claims of the '759 Patent (24 pages)	
	D1156	Exhibit 263, Wang vs. Claims of the '135 Patent (59 pages)	
	D1157	Wang vs. Claims of the '504 Patent (55 pages)	
	D1158	Wang vs. Claims of the '211 Patent (56 pages)	
	D1159	Exhibit 1, Alexander CV (22 pages)	
	D1160	Exhibit 2, Materials Considered by Peter Alexander (16 pages)	
	D1161	Exhibit 3, Cross Reference Chart (24 pages)	
	D1162	Exhibit 4, RFC 2543 vs. Claims of the '135 Patent (43 pages)	
	D1163	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent (46 pages)	
	D1164	Exhibit 6, RFC 2543 vs. Claims of the '211 Patent (46 pages)	
	D1165	Exhibit 7, The Schulzrinne Presentation vs. Claims of the '135 Patent (32 pages)	
	D1166	Exhibit 8, The Schulzrinne Presentation vs. Claims of the '504 Patent (36 pages)	
	D1167	Exhibit 9, The Schulzrinne Presentation vs. Claims of the '211 Patent (36 pages)	
	D1168	Exhibit 10, The Schulzrinne Presentation vs. Claims of the '151 Patent (15 pages)	
	D1169	Exhibit 11, The Schulzrinne Presentation vs. Claims of the '180 Patent (11 pages)	
	D1170	Exhibit 12, The Schulzrinne Presentation vs. Claims of the '759 Patent (29 pages)	
	D1171	Exhibit 13, SSL 3.0 vs. Claims of the '135 Patent (33 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	51	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1172	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent (38 pages)	
	D1173	Exhibit 15, SSL 3.0 vs. Claims of the '211 Patent (39 pages)	
	D1174	Exhibit 16, SSL 3.0 vs. Claims of the '151 Patent (10 pages)	
	D1175	Exhibit 17, SSL 3.0 vs. Claims of the '759 Patent (25 pages)	
	D1176	Exhibit 18, Kiuchi vs. Claims of the '135 Patent (30 pages)	
	D1177	Exhibit 19, Kiuchi vs. Claims of the '504 Patent (35 pages)	
	D1178	Exhibit 20, Kiuchi vs. Claims of the '211 Patent (35 pages)	
	D1179	Exhibit 21, Kiuchi vs. Claims of the '151 Patent (8 pages)	
	D1180	Exhibit 22, Kiuchi vs. Claims of the '180 Patent (19 pages)	
	D1181	Exhibit 23, Kiuchi vs. Claims of the '759 Patent (25 pages)	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401 vs. Claims of the '135 Patent (51 pages)	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '504 Patent (45 pages)	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '211 Patent (45 pages)	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '151 Patent (18 pages)	
	D1186	Exhibit 28 (2 pages)	
	D1187	Exhibit 29, The Altiga System vs. Claims of the '135 Patent (35 pages)	
	D1188	Exhibit 30, The Altiga System vs. Claims of the '504 Patent (40 pages)	
	D1189	Exhibit 31, The Altiga System vs. Claims of the '211 Patent (41 pages)	
	D1190	Exhibit 32, The Altiga System vs. Claims of the '759 Patent (35 pages)	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '135 Patent (64 pages)	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '504 Patent (39 pages)	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '211 Patent (41 pages)	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '151 Patent (19 pages)	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '180 Patent (33 pages)	
	D1196	Exhibit 38, Kent vs. Claims of the '759 Patent (17 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	52	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent (48 pages)	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent (48 pages)	
	D1199	Exhibit 41, Aziz ('646) vs. Claims of the '759 Patent (24 pages)	
	D1200	Exhibit 42, The PIX Firewall vs. Claims of the '759 Patent (24 pages)	
	D1201	Exhibit A-1, Kiuchi vs. Claims of the '135 Patent (181 pages)	
	D1202	Exhibit B-1, Kiuchi vs. Claims of the '211 Patent (200 pages)	
	D1203	Exhibit C-1, Kiuchi vs. Claims of the '504 Patent (278 pages)	
	D1204	Exhibit D, Materials Considered (3 pages)	
	D1205	Exhibit E, CV of Stuart G. Stubblebine, Ph.D (19 pages)	
	D1206	Exhibit F, Claim Construction Chart (7 pages)	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents (60 pages)	
	D1208	Cisco Comments and Petition for Reexamination in Control No. 95/001,679 dated June 14, 2012 (69 pages)	
	D1209	Exhibit S, Declaration of Nathaniel Polish, Ph.D in Control No. 95/001,679 (5 pages)	
	D1210	Exhibit R, Excerpts from Patent Owner & Plaintiff VimetX Inc. 's First Amended P.R. 3-1 and 3-2 Disclosure of Asserted Claims and Infringement Contentions (53 pages)	
	D1211	Third Party Requester Comments dated June 25, 2012 - After Non Final Office Action in Control No. 95/001,788 (37 pages)	
	D1212	Reexam Affidavit/Declaration/Exhibit Filed by 3rd Party on June 25, 2012 in Control No. 95/001,788 (19 pages)	
	D1213	Extended European Search Report dated 03/26/12 from Corresponding European Application Number 11005793.2 (077580-0144) (6 pages)	
	D1214	Bergadano, et al., "Secure WWW Transactions Using Standard HTTP and Java Applets," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998 (12 pages)	
	D1215	Alexander Invalidity Expert Report dated May 22, 2012 with Exhibits (1542 pages)	
	D1216	Transcript of Deposition of Peter Alexander dated July 27, 2012 (55 pages)	
	D1217	Cisco '151 Comments by Third Party Requester dated August 17, 2012 with Exhibits (211 pages)	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dated August 17, 2012 (4 pages)	
	D1219	Transcript of August 22, 2012 Deposition of Stuart Stubblebine (69 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

PATENT
Customer No. 23,630
Attorney Docket No. 077580-0160

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,949
U. S. Patent No. 8,051,181	Group Art Unit: 3992
Issued: November 1, 2011	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.550 and M.P.E.P. § 2266.03, the undersigned attorney for the patent owner certifies that a copy of the Information Disclosure Statement, PTO Form SB/08, and listed references C8, C19, C21, C24, and D257, D258, D259, D261, D263, D264, D266, and D292-D1219 was served by first-class mail on September 20, 2012, on counsel for the third party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Dated: September 20, 2012

By: /Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
McDermott Will & Emery LLP
Attorney for Patent Owner

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com

Please recognize our Customer No. 23630 as our correspondence address.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

23630 7590 09/21/2012
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
09/21/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

MCDERMOTT WILL & EMERY
600 13TH STREET, NW
WASHINGTON, DC 20005-3096

(For Patent Owner)

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

(For Third Party Requester)

Inter Partes Reexamination Proceeding
Control No. 95/001,949
Filed: March 28, 2012
For: U.S. Patent No. 8,051,181

DECISION
GRANTING
PETITION

This is a decision on patent owner's September 4, 2012 petition entitled "PETITION SEEKING WAIVER OF 37 C.F.R. § 1.943 FOR PATENT OWNER'S RESPONSE TO OFFICE ACTION OF JUNE 4, 2012."

The petition under 37 CFR 1.183 is before the Office of Patent Legal Administration.

The petition under 37 CFR 1.183 is **granted** to the extent set forth herein.

RELEVANT BACKGROUND

1. On November 1, 2011, U.S. patent number 8,051,181 (the '181 patent) issued to Larson *et al.*

2. On March 28, 2012, a third party requester filed a request for *inter partes* reexamination of the '181 patent, which request was assigned Reexamination Control No. 95/001,949 (the '1949 proceeding). Apple Inc. is identified as the real party in interest.

3. On June 4, 2012, the Office issued an order granting *inter partes* reexamination in the '1949 proceeding along with a Non-Final Rejection.

4. On September 4, 2012, patent owner filed a petition entitled "PETITION SEEKING WAIVER OF 37 C.F.R. § 1.943 FOR PATENT OWNER'S RESPONSE TO OFFICE

ACTION OF JUNE 4, 2012" (petition under 37 CFR 1.183), concurrently with a response submission.[1]

DECISION

I. Relevant Statutes, Regulations and Procedures

37 CFR 1.183 provides:

> In an extraordinary situation, when justice requires, any requirement of the regulations in this part which is not a requirement of the statutes may be suspended or waived by the Director or the Director's designee, *sua sponte*, or on petition of the interested party, subject to such other requirements as may be imposed. Any petition under this section must be accompanied by the petition fee set forth in § 1.17(f).

37 CFR 1.943(b) provides:

> Responses by the patent owner and written comments by the third party requester shall not exceed 50 pages in length, excluding amendments, appendices of claims, and reference materials such as prior art references.

II. Discussion

37 CFR 1.183 provides for suspension or waiver of any requirement of the regulations which is not a requirement of the statutes in an extraordinary situation, when justice requires, on petition of the interested party. The burden is on petitioner to set forth with specificity the facts that give rise to an extraordinary situation in which justice requires suspension of a rule. A showing which petitioner can make in support of a request for waiver of the 50-page limit of 37 CFR 1.943(b) can be an attempt to draft a patent owner's response or third party requester comments submission in compliance with the 50-page limit, and submission of a resulting response or comments submission that is in excess of 50 pages concurrently with a petition under 37 CFR 1.183 for waiver of 37 CFR 1.943(b), requesting entry of the proposed submission. Such a response or comments submission can be evaluated for economizing, extraneous material, and arrangement, without repetition of information already of record. In this way, petitioner can rely on the proposed response or comments submission: (1) for justification that more pages are needed to complete the response, and (2) to set forth an accurate determination of exactly how many additional pages petitioner deems to be needed for the response or comments submission.

It is noted that, for purposes of making an accurate determination of exactly how many additional pages over 50 are deemed to be needed for the response, a document is deemed to be subject to the 50-page length requirement when the document includes legal argument, *i.e.*, arguments of counsel such as, *e.g.*, arguments that the claims are patentable or unpatentable, or

[1] On June 27, 2012, the Office mailed a decision granting a one-month extension of time for patent owner's response to the June 4, 2012 Office Action.

that are directed to how an outstanding or proposed rejection is overcome, or, in the case of a document filed by the requester, how an outstanding or proposed rejection is supported. Each determination of whether a document, such as an affidavit or declaration, contains information that will cause the document to be subject to the page count is made on a case-by-case basis. In determining whether a document such as an affidavit or declaration under 37 CFR 1.132, or any other document of a submission, includes legal argument, the Office analyzes whether the document is providing factual evidence, *i.e.*, evidence of **technological facts,** or whether the document contains argument that is merely an extension of the arguments of counsel. Factual evidence includes, for example, declarations that swear behind the filing date of a reference, that establish the date of a printed publication, that provide a technical explanation or technical definition of terms of art used by a reference, or that provide comparative test results and a scientific, or technological, analysis of the results (*see*, *e.g.*, MPEP 716.02). If a document is limited to factual evidence, the document is not included in the page count. In addition, affidavits or declarations limited to establishing commercial success, long-felt need and failure of others, scepticism of experts, or copying, as per MPEP 716.03-716.06, respectively, will not be included in the page count.

III. Patent owner's petition under 37 CFR 1.183

On September 4, 2012, patent owner filed the instant petition under 37 CFR 1.183, requesting waiver of 37 CFR 1.943(b) to permit entry of its concurrently-filed response submission. Patent owner asserts that the September 4, 2012 response submission is 78 pages long, excluding amendments, appendices of claims, and reference materials.[2] Patent owner states that it also submitted two declarations, one by one of the inventors (Dr. Short) and another by an expert (Dr. Keromytis), but asserts that "[t]he declaration of Dr. Short presents facts regarding secondary considerations and the declaration of Dr. Keromytis discusses how one of ordinary skill in the art would have understood the references cited in the Office Action." Patent owner asserts that it believes neither declaration should count towards the page limit.[3] Nonetheless, patent owner requests waiver of the 50-page limit to submit these declarations with its response "should the Office decide to include portions of either declaration in the page count for the response...."[4]

In support of its request for waiver of the rule, patent owner asserts that the Office action adopted eleven grounds of rejection and "the Examiner incorporated by reference corresponding portions of the 319 pages of Apple's request and 49 pages of accompanying claim charts."[5] Patent owner asserts that it "has made every effort to pare down its response," but that "limiting its response to 50 pages would severely compromise its ability to fully address the issues raised in the Office Action."[6] Patent owner further asserts that "even if the Office were to count the declarations towards the page limit, the total number of pages representing the response and the declarations would still be substantially less than the 319 pages of Apple's request and 49 pages of accompanying claim charts relied upon and incorporated by reference in the Office Action."[7]

[2] Patent owner petition under 37 CFR 1.183 at page 1.
[3] Id.
[4] Id.
[5] Id. at pages 2-3.
[6] Id. at page 2.
[7] Id..at page 3.

Based on the specific facts set forth in patent owner's petition under 37 CFR 1.183, patent owner's showing in support of the request for waiver of the 50-page limit of 37 CFR 1.943(b) by attempting to draft a response in compliance with the 50-page limit and submitting the resulting response (which is in excess of 50 pages),[8] and the individual facts and circumstances of this case (such as the length of the June 4, 2012 Office action),[9] it is deemed equitable to waive the 50-page limit of 37 CFR 1.943(b) in this instance. Accordingly, patent owner's petition under 37 CFR 1.183 is granted and the page limit of 37 CFR 1.943(b) is waived to the extent necessary to permit entry of patent owner's September 4, 2012 response submission. This waiver makes patent owner's September 4, 2012 response submission page-length compliant.

CONCLUSION

1. Patent owner's September 4, 2012 petition under 37 CFR 1.183 is **granted** and the 50-page limit of 37 CFR 1.943(b) is waived to the extent necessary to permit entry of patent owner's May 15, 2012 response submission. This waiver makes patent owner's May 15, 2012 response submission page-length compliant.

2. Any questions concerning this communication should be directed to Nicole D. Haines, Legal Advisor, at (571) 272-7717.

Pinchus M. Laufer
Senior Legal Advisor
Office of Patent Legal Administration

09-19-2012

[8] 78 pages of the remarks portion of patent owner's September 4, 2012 response submission count toward the regulatory page limit (the cover page and pages of the table of contents are excluded from the page count). Thus, the patent owner's September 4, 2012 response submission exceeds the 50-page limit by at least 28 pages, without including any portions of the 6-page Short declaration and 45-page Keromytis declaration that also count toward the regulatory page limit.

[9] On its face, the June 4, 2012 Office action spans only 13 pages but, in setting forth the proposed rejections that have been adopted, incorporates by reference approximately 350 pages from the '1949 request for *inter partes* reexamination, exceeding the number of pages of patent owner's proposed response, including any pages of the accompanying declarations that also count toward the regulatory page limit.

Attorney Docket No. 41484-80120

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of	)	
U.S. Patent No. 8,051,181	)	Control No.: 95/001,949
Victor Larson et al.	)	Group Art Unit: 3992
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. § 1.947

Mail Stop **Inter Partes Reexam**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On September 4, 2012, Patent Owner filed an overlength response ("Response") to the June 4, 2012 Office action ("Office Action") and a petition under 37 C.F.R. § 1.183 seeking waiver of the page limit for that response. On September 21, 2012, the Office granted Patent Owner's petition, which set the date for a response by the Requestor for 30 days from the date of decision, which fell on Sunday, October 21, 2012. This response is timely filed on the next business day, Monday, October 22, 2012. *See* 35 U.S.C. § 21. Third Party Requester believes that no fee is due in connection with the present response. However, any fee determined to be required for entry or consideration of this paper may be debited from Deposit Account No. 18-1260.

- A table of contents is provided on pages ii to v.[1]
- The response to the Patent Owner Comments begins on page 1.

[1] Requester submits that pages corresponding to a table of contents are not to be counted against the page limits applicable to this response. Should the Office determine otherwise, it is requested to disregard the table of contents if doing so renders this Response overlength.

Table of Contents

I. Introduction

Requestor urges the Examiner to maintain the rejections of claims 1-29 set forth in the Office Action dated June 4, 2012 (the "Office Action").

II. Response to Patent Owner Contentions on Status of References as Prior Art.

On pages 4-6 of the Response, Patent Owner asserts there is no evidence that *Lendenmann, H.323, H.225.0, H.235, H.245* and "RFCs" are prior art under 35 U.S.C. § 102(a) or (b). Patent Owner's claims are frivolous – each reference is unquestionably a printed publication, and only by studied ignorance of the facts can Patent Owner assert otherwise. Regardless, evidence was presented with the Request or is provided below that unequivocally establishes that each of *Lendenmann, H.323, H.225.0, H.235, H.245* and "RFCs" documents was publicly disseminated before February 15, 2000, and thus is prior art to the '181 patent.[2]

The *Lendenmann* reference, "Understanding OSF DCE 1.1 for AIX and OS/2," ("*Lendenmann*") was published by the IBM International Technical Support Organization in October 1995—well in advance of the earliest available priority date of the '181 patent, and is therefore unquestionably prior art under 35 U.S.C. § 102(b). Indeed, as indicated on its face, the *Lendenmann* reference was published in October 1995 as part of IBM's well known "redbook" collection. It was cataloged as redbook number SG24-4616 and, as described on page xxi, was made publicly available on the Internet at: http://www.redbooks.ibm.com/redbooks. As further evidence of its publication, the Internet Archive ("the Wayback Machine") shows that the document was publically available on the IBM website no later than December 3, 1998, as indicated on Exhibit A. As provided in M.P.E.P. § 2128, "[a]n electronic publication, including an on-line database or Internet publication, is considered to be a 'printed publication' within the meaning of 35 U.S.C. 102(a) and (b) provided the publication was accessible to persons concerned with the art to which the document relates." The *Lendenmann* reference therefore is a printed publication and § 102(b) prior art to the '181 patent.

Patent Owner next asserts that the *H.323* and associated core recommendations are printed publications. Response at 5-6. This is a baseless challenge. The ITU-T *H.323* Core Recommendations are a series of protocols that are published by the ITU Telecommunication Standardization Sector (ITU-T)—an organization that dates back to 1865—whose mission is to

[2] Patent Owner does not contest Requester's assertions on page 12 of the Request that the effective filing date of the '181 patent was no earlier than April 20, 2000.

ensure the efficient and timely availability of standards deemed essential to the telecommunications industry. The face of these documents shows they were approved and made available publically no later than February of 1998. As further evidence, the Wayback Machine shows that the recommendations were posted to the ITU website no later than August 3, 1998. Exhibit B. Thus, each of the *H.323, H.225.0, H.235, H.245* recommendations was publically disseminated and is prior art to the 181 patent.

Patent Owner also asserts that several Request for Comment (RFC) documents are printed publications, claiming that "the record is devoid of evidence that any of these references are … printed publications as of" each publication date listed on each RFC. This too is a frivolous challenge – RFC documents are published and disseminated to the public by the Internet Engineering Task Force (IETF) pursuant to transparent and well-known procedures. Specifically: (i) each number assigned to an RFC is unique and is not "re-used" if the subject matter in an RFC is revised or updated, (ii) the date each RFC is distributed to the public is listed the front page of the RFC, (iii) RFCs are distributed to the public over the Internet, via numerous protocols, (iv) each RFC is announced via an email distribution list on the date it is released to the public, and (v) RFCs are maintained in numerous archives publicly accessible via the Internet. In fact, Patent Owner itself cites several RFCs as "printed publications" in the '181 patent. Patent Owner thus cannot seriously contend that RFCs are not publicly disseminated.

Patent Owner's frivolous assertions about the status of these documents as printed publications should not be countenanced, and signal their relevance to the patent claims.

III. The Rejections Of the Claims Were Proper And Should Be Maintained

Claims are given "their broadest reasonable interpretation, consistent with the specification, in reexamination proceedings." *In re Trans Texas Holding Corp.*, 498 F.3d 1290, 1298 (Fed. Cir. 2007). In determining that meaning "it is improper to 'confin[e] the claims to th[e] embodiments' found in the specification." *Id.* at 1299 (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (*en banc*)). While "the specification [should be used] to interpret the meaning of a claim," the PTO cannot "import[] limitations from the specification into the claim." *Id.* "A patentee may act as its own lexicographer and assign to a term a unique definition that is different from its ordinary and customary meaning; however, a patentee must *clearly* express that intent in the written description." *Helmsderfer v. Bobrick Washroom Equip., Inc.*, 527 F.3d 1379, 1381 (Fed. Cir. 2008) (emphasis added). No express definitions of key claim terms is provided in the

'181 patent (e.g, secure name, secure name service, unsecure name, and registration). Thus, these terms must be given their broadest reasonable interpretation in these reexamination proceedings.

A. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-12, 14, 15, and 17-29 Based on *Beser* (Issue 1).

1. Independent Claim 1

The Examiner correctly found that *Beser* describes a system that anticipates claim 1. In response, Patent Owner asserts *Beser* does not teach a system that discloses (1) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device," (2) "the claimed 'first device' and 'second device,'" and (3) "sending a message over a secure communication link." Response at 7-12. Each of these is incorrect.

a. *Beser Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"*

Patent Owner elects to start its response to this rejection by asserting that Requester "...never expressly identifies the elements of *Beser* that allegedly qualify as the claimed 'message.'" Response at 7. However, the Request clearly explained how *Beser* describes each element of claim 1. Request at 24-31. By electing to criticize how the Requester demonstrated that *Beser* anticipates claim 1, Patent Owner reveals the frailty of its position.

Patent Owner's criticisms are substantively pointless – *Beser* plainly describes "messages" specified in claim 1. Certainly, Patent Owner cannot seriously contend that the transmissions being sent in the Beser systems are not "messages." For example, the description of Figure 6 in *Beser* (which is prominently displayed in the Request to illustrate how claim 1 is anticipated) explains that it is "a block-diagram illustrating the <u>**message**</u> flow." *Beser* at 3:30-32.

Patent Owner next presents a series of convoluted explanations why the messages in *Beser* are not "messages" handled as required by the claims. Initially, Patent Owner's arguments presume that the claims impose substantive restrictions on the form, handling or content of these-- they do not. Instead, claim 1 reads simply:

- receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired [sic] to securely communicate with the first device; and
- sending a message over a secure communication link from the first device to the second device.

Response at 7-8. As is evident from the claim language, a message can be any form of a communication received at a network address "corresponding to the secure name associated with the first device" that indicates a communication is "desired" by a second device.

To assert that *Beser* does not describe this step, Patent Owner presents an obviously incorrect portrayal of both the claim requirements and the *Beser* procedures. Specifically, at pages 6-7, Patent Owner presents a rambling discussion about whether an originating telephony device or a first network device can be a "first device" which receives a "message" according to the claims. Patent Owner theorizes that the "originating telephony device" in Figure 6 of Beser could be the "first device" of the claims, which, in the mind of the Patent Owner, would require the "second device" in the claims to be the "first network device" in Beser. *See Id.* at 7. The claims, however, do not delineate *how* a request must be transported or received, or, for that matter what a "first device" may comprise. They also do not restrict which of several devices in a path of communications may be the "first" or "second" device. Thus, the telephony, network devices (e.g., edge routers) and/or trusted third party network device described in *Beser* may, at any particular point, be a "first" or "second" device in the claims. What Patent Owner cannot contest is that *Beser* shows that *messages* are sent and *received* by devices that correspond to the secure name associated with the corresponding device (e.g., the private IP address of the other device). Patent Owner's theory that messages cannot be sent via intervening devices is refuted by its own disclosure, which show analogous deployments to those in *Beser*. As the '181 patent explains: "... a first computer 2401 communicates with a second computer 2402 **through two routers** 2403 and 2404. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks)." '181 Patent at col.37, ll.65-69; *see also* Fig. 24. Patent Owner's incorrect and irrelevant comments about messages in *Beser* should be disregarded.

b. *Beser Discloses the Claimed "First Device" and "Second Device."*

Patent Owner next asserts that *Beser* fails to disclose a "first device" and a "second device" according to the claims. Again, Patent Owner starts by attacking the *form* of <u>the Request</u> (i.e., that it "never expressly identifies" the first and second devices). Of course this is incorrect – Patent Owner actually discusses the part of the Request that describes how *Beser* anticipates this feature of the claims. Request at 24-31.

Patent Owner then contests that *Beser* shows a first and second device. First, Patent

Owner theorizes that whether the "[f]irst and second network devices (14, 16) and end-point devices (24, 26) have associated therewith both secure and unsecure names" means that Requester is implying "that *four* different devices in *Beser* disclose the recited 'first device' and 'second device.'" How Patent Owner can reach this conclusion from either the Request or the teachings in *Beser* cannot be deciphered. In reality, *Beser* shows a system where the private IP address of a second edge router and/or telephony device is in a message provided to the first router/telephony device. This meets the requirements of the claims. It also is immaterial whether the "first device" is considered to be the telephony device, the edge router or both working together – there is no restriction on the claims to this extent. Instead, of addressing what is literally described in *Beser*, Patent Owner elects to focus on a hypothetical reading of *Beser* and whether Request adequately points out the relevant teachings in *Beser*. The Examiner apparently had no difficulty recognizing that the end-point devices (24, 26) in *Beser* — which are positioned just like the computers (2401, 2402) of the '181 patent—are the claimed "first" and "second" devices. Patent Owner's other assertion simply repeats its incorrect theory that *Beser* does not disclose a "message."

c. *Beser Discloses "Sending a Message Over a Secure Communication Link."*

The Examiner correctly found that *Beser* discloses "sending a message over a secure communication link." In response, Patent Owner asserts that *Beser* does not describe a "secure communication link" because (1) "the broadest reasonable interpretation of secure communication link requires encryption, and *Beser's* tunneling association is not encrypted" and (2) "even if the Office determines that a secure communication link does not require encryption, *Beser*'s tunneling associate still is not a secure communication link." Response at 10. Both points are incorrect.

Contrary to Patent Owner's assertions, the claims read in their broadest reasonable construction do not require encryption. Specifically, the term "secure communication link" is not expressly defined in the claims or the specification to require encryption. Thus, Patent Owner's contention that one of ordinary skill would understand *Beser* to "provide[] an alternative to establishing" a secure communication link is simply incorrect. Rather, as the Patent Office found recently in reexamination of a related VirnetX patent, one of ordinary skill would not find the language "secure communication link to [require] encrypt[ion]." Action Closing Prosecution of

95/001,788 ("'788 ACP") at 33.[3] In fact, the Patent Office explained that "*Beser* teaches an unsecured Internet link can be secured by means other than encryption, such as hiding the source address so that the users cannot be mapped to a source address. Encryption is more secure than hiding the source address just as encryption and hiding the address is more secure than encryption only. The claim however do not recite the degree of security." *Id.*

Moreover, *Beser* does not state that encryption should never be used in IP tunneling schemes. Instead, *Beser* consistently and repeatedly points out that encryption in IP tunneling schemes (of which its system is one) is conventional and ordinarily should be used. *Beser* at col.1, ll.54-56 ("Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ('IPSec').") In fact, *Beser* specifically refers to *Kent* (the RFC describing the IPSec protocol) to explain how encryption is conventionally incorporated into IP tunneling schemes. Certainly, *Beser* does indicate that certain applications may raise practical challenges in using encryption in IP tunneling schemes – particularly, "VOIP and multimedia." However, this concern is not an express teaching (as Patent Owner contends) to never use IPSec or other encryption-based IP tunneling models, or that the *Beser* techniques are an alternative to using encryption— a conclusion in which the Patent Office expressly agrees. '788 Order at 32. Instead, *Beser* points out that these practical concerns do not always arise for these two data types, and do not arise at all for data transfer scenarios other than those two types. As *Beser* explains, even in these two high data volume applications, encryption should generally be used. *Beser* at col.2, ll.12-14 (indicating that in a particular VOIP system that uses a VPN, "the tunneled IP packets, however, may need to be encrypted before encapsulation in order to hide the source IP address."). *Beser*, thus, teaches the person of ordinary skill that encryption ordinarily should be used in IP tunneling applications, not, as Patent Owner contends, that it should not. *Beser* at col.1, ll. 54-66. And, critically, none of the claims are restricted to implementations requiring high data volume applications that were the target of the cautionary statements in *Beser*. Thus, these cautionary observations are entirely irrelevant to the '181 claims and consequently, Patent Owner's analysis.

Patent Owner next contends that "even if the Office determines that a secure communication link does not require encryption"—which, as described above, the Office has—then "*Beser's* tunneling association still is not a secure communication link." Response at 12.

[3] U.S. Patent No. 7,418,504 to Larson, which is at issue in the '788 reexamination, is derived from the same applications as U.S. Patent No. 8,051,181 to Larson, the patent at issue here.

But the Patent Office has already determined that this statement is incorrect too. Indeed, the Patent Office explains that "the patent owner misunderstand *Beser.*" '788 ACP at 32. Requester agrees. Rather than teaching away from a secure communication link, as Patent Owner contends, "*Beser* teaches its tunneling invention efficiently solves the problem of encrypted IP packets with readable source addresses." *Id.* As explained in the Request, the inventive tunneling method of *Beser* "is designed to protect the integrity of the private IP address and ensure the anonymity of the terminating devices." Request at 26. The solution of *Beser* is thus a distinct layer of security because IPsec encrypted IP packets, for example, cannot conceal the identity of the source addresses. *Id.* at 26-29; *see also*'788 ACP at 32. Accordingly, "Beser discloses a secure communication link." '788 ACP at 32.

2. Independent Claim 2

The Examiner correctly found that *Beser* discloses every limitation of dependent claim 2. In response, Patent Owner contends only that the "trusted-third-party network device 30" of *Beser* does not disclose a "secure name service" because it "omits any description of how the trusted-third-party network device is associated with any form of security." Response at 12-13. This is plainly incorrect. As explained in the Request, *Beser* teaches that "the end-point devices (24, 26) each have a secure name that comprises a 'unique identifier' that is registered with the trusted-third party device," and further that the "association of the public IP address for [a network device] with the unique identifier is made on the trusted-third-party network device 30." Request at 32. Further, Patent Owner made representations during the prosecution of the related '180 patent as to the construction of the terms "secure name" and "secure name service," which was noted by the Examiner. Order at 5. In particular, Patent Owner explained that a "*'secure name' is a name associated with a network address associated of a [SIC] first device. The name can be registered such that a second device can obtain the network address associate with the first device from a secure name registry and send a message to the first device.*" Order at 5 (emphasis added). The Patent Owner's comments are thus instructive of the broadest reasonable construction of the term "secure name service," and under such a construction, the trusted-third-party network device discloses this only disputed limitation of the claim. Accordingly, the Examiner's finding of anticipation of claim 2 was proper and should be maintained.

3. Dependent Claims 3-4, 8, 12, 14-15, 17 and 19-22

Patent Owner presents no distinct response to the rejection of claims 3-4, 8, 12, 14-15, 17 and 19-22 based on *Beser* relative to its response to the rejection of claim 2. Consequently, because the rejection of those claims was proper, the Examiner's rejection of claims 3-4, 8, 12, 14-15, 17 and 19-22 based on *Beser* was proper and should be maintained. Request at 35-37, 39, 41, 43, 44-45.

4. Dependent Claim 5

The Examiner correctly found that *Beser* anticipates every limitation of dependent claim 5. Patent Owner responds that the tunneling association of *Beser* does not include "receiving a message in encrypted form," as the techniques disclosed in *Beser* teach encryption techniques "only to the extent that they should *not* be used in tunneled connections and other VoIP applications." Response at 13. Patent Owner's analysis of *Beser* is incorrect for many of the reasons already stated. Request at 36-37. The Patent Owner also ignores the disclosures in *Beser* that show that encryption is, in fact, used in the *Beser* DNS systems. Specifically, *Beser* teaches that queries involving the unique identifier [e.g., a domain name] may be encrypted. *Beser* at col.11, ll.22-25 ("The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12."). *Beser* thus clearly teaches that encryption can be used in various ways to support secure communication links (e.g., use of IPSec-compliant systems, use during negotiation and establishment of the secure communication link).

Patent Owner also asserts that *Beser* does not disclose the claimed "message containing the network address." Response at 13. For the same reasons already discussed above in section A(1)(a), this argument is incorrect and should be disregarded. Consequently, the Examiner's rejection of this claim was proper and should be maintained.

5. Dependent Claim 6

The Examiner correctly found that *Beser* discloses all the limitations of dependent claim 6. In response, Patent Owner alleges only that the rejection fails to identify "a single feature in *Beser* in which decrypting the message would be necessarily present." Response at 14. Patent Owner's response is meritless, as it ignores the unambiguous disclosure of the encryption of IP packets in *Beser*, as discussed repeatedly above, which, to be functional, inherently require decryption of those packets. *See also* Request at 37. Thus, *Beser* necessarily discloses "decrypting the message." Accordingly, the Examiner's rejection as imposed was proper and should be maintained.

6. Dependent Claim 7

The Examiner correctly found that *Beser* discloses a system "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." As the Request explains, *Beser* shows that the disclosed standards-based system that includes first and second network devices (14, 16) and endpoint devices (24, 26) are designed (i.e., are capable) to interact with the numerous standards proposed by the IETF, and any other network-based standards. Request at 37. Patent Owner responds only that "additional explanation" is needed and that the standards identified in *Beser* have not "properly been incorporated by reference." Response at 14. First, no additional explanation is necessary—claim 7 only requires that the disclosed system be "capable" of supporting a non-secure communication link." Moreover, *Beser* clearly explains that its preferred embodiment includes devices "that can interact with network system[] based on standards proposed by" IEEE, ITU, IETF, or WAP, for example. *Beser* at col.4, ll.55-63. Such standards—which were well-known to one skilled in the art prior to February of 2000 —would include those "capable" of supporting non-secure communication links. Second, it is not necessary that *Beser* incorporate the proposed standards—all that is necessary is that *Beser* explains that the disclosed systems are capable of supporting such standards, which *Beser* has done. Thus, contrary to Patent Owner's assertion, *Beser* discloses a system that anticipates claim 7, and the Examiner's rejection was proper.

7. Dependent Claim 9

The Examiner correctly found that *Beser* discloses "automatically initiating the secure communication link after it is enabled." In Response, Patent Owner argues that *Beser* does not disclose "automatically initiating the secure communication link" as it is silent on that feature. Response at 14-15. Patent Owner is apparently relying on the literal absence of the two words in sequence ("automatically initiating") in *Beser* as a basis for its assertions. This is because *Beser* plainly does show initiation of a secure communication link upon completion of the negotiation process between networked devices, and that this occurs without user intervention (i.e., a meaning within the scope of the terms "automatically initiating"). Request at 38. For example, *Beser* explains that, in response to a request containing a unique identifier specifying the location of a second network device, the trusted-third-party network device will negotiate with first and second network devices to establish an IP tunnel between the first and second network devices. *Beser* further explains that the "negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26)." *Id.* at col. 12, ll. 6-19. The private network IP addresses are then used in conjunction with the public IP addresses of the first and second network devices to establish the tunnel (i.e., the secure communication link) automatically between the first and second network devices. *See id.* at col.12, ll. 28-37. These steps occur without any interaction from the user that originally made the request. Thus, as the Request explained, the *Beser* processes are "automatic" and transparent to the user. The rejection of claim 9 was, consequently, proper.

8. Dependent Claim 10 and 11

The Examiner correctly found that *Beser* discloses each of the limitations of claims 10 and 11. Claim 10 includes the requirement of "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 includes the requirement of "receiving the message in the form of at least one tunneled packet." As the Request explains, each of these claims is satisfied by *Beser*'s disclosure of a tunneling technique designed to obfuscate the identity of the source and destination addresses of a secure communication link. Request at 38. Patent Owner contends that the Request only identifies "what Requester alleges to be the secure communication link, not the alleged 'message containing the network address.'" Response at 15. Patent Owner also asserts that the identified "tunneling" is "not directed to the alleged 'message containing the network address.'" *Id.* These responses simply ignore the contents of *Beser*, which clearly explains that the disclosed security measures may be performed through "initiating and maintaining a virtual tunnel." *Beser* at col.6, ll.58-59. *Beser* further explains the importance of protecting the negotiation process—which comprises messages "containing the network address associated with the secure name of the device"—from hackers. Request at 38. As one goal of *Beser* is the protection of the identities of the source addresses, it would be illogical to create the tunneling association only <u>after</u> the VoIP connection has been established. Accordingly, the Examiner's rejection of these claims was proper and should be maintained.

9. Dependent Claim 18

The Examiner correctly found that *Beser* discloses every limitation of dependent claim 18. In response, Patent Owner contends that authentication described in *Beser* has nothing "to do with the alleged secure communication link." Response at 15. Patent Owner is incorrect. Request at 43-44. The Request explains that the IP 58 packets that comprise the negotiation process "may require encryption and authentication to ensure that the unique identifier cannot be read on the public network." *Beser* at col.11, ll.22-24. This is the negotiation process that facilitates the establishment of the secure communication link, and the failure of this authentication step would necessarily preclude the establishment of the secure communication link. Patent Owner's comments thus rest on an assumption that is technically incorrect. Accordingly, the Examiner's rejection of claim 18 was proper and should be maintained.

10. Dependent Claim 23

The Examiner correctly found that *Beser* discloses every limitation of dependent claim 23. Patent Owner responds that "*Beser* does not disclose that the unique identifier (referred to as a "domain name") is a non-standard domain name. Response at 16. Patent Owner is incorrect, as it ignores its own representations of the term "non-standard domain name" during prosecution of the '180 patent. Request at 45; Order at 5. There, the Patent Owner explained that a "'secure name' can be a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number." *Id.* As explained in the Request, the "unique identifier is any of a dial-up number, an electronic mail address, or a domain name." Request at 45. Consequently, the Examiner's rejection of claim 18 was appropriate and should remain.

11. Independent Claim 24

The Examiner correctly found that *Beser* describes a method using a first device to securely communicate with a second device over a communication network in the manner described in claim 24. In response, the only new argument that Patent Owner presents is that there is "simply no evidence" that the limitation of "'at the first device requesting and obtaining registration of a secure name for the first device' is necessarily present in *Beser* to support an inherency theory." Response at 16. This is incorrect. The Request explains that "the trusted-third-party network device 30 may be a directory service . . . that retains a list of E.164 numbers for its subscribers." Request at 46. Such a list is only possible if the devices request and obtain registration of their respective secure names.

Patent Owner presents no other response to the rejection of claim 24 with respect to any of its other limitations and instead relies on those allegations "similar to those given in support of the patentability of claim 1." Because the rejection of claim 1 was proper, the rejection of claim 24 based on *Beser* should be maintained.

12. Claims 25-29

In response to the rejection of claims 25-29, Patent Owner presents no distinct responses from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claims 25-29 based on *Beser* were also proper and should also be maintained. *See also* Request at 50-65.

B. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1, 2, 6-9, 12-17, and 24-29 Based on *Mattaway* (Issue 3).

1. Independent Claim 1

The Examiner properly found that *Mattaway* describes a system that anticipates claim 1. In response, Patent Owner asserts *Mattaway* does not teach a system that discloses (1) "[a] first device associated with a secure name and an unsecured name" (2) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, (3) "sending a message over a secure communication link from the First Device to the Second Device." Response at 20-22. Each assertion is incorrect.

a. *Mattaway Discloses "A First Device Associated With A Secure Name and An Unsecured Name"*

Patent Owner asserts that *Mattaway* "does not disclose that the email address in Table 9 is associated with any particular device, much less the alleged callee's device." Response at 20. Patent Owner also argues that "*Mattaway* is completely silent as to the function of the referenced email address." Response at 20. Each point is incorrect. Request at 69. In the same section referenced by Patent Owner, *Mattaway* explains that the data in Table 9—which includes the encrypted email address "eemailAddr" entry—is used by global server 1500 "in the event that the WebPhone client process is logging on for the first time" in order to register certain information from that particular new WebPhone client. *Mattaway* at col.22, ll.65-59. *Mattaway* thus discloses that information requested from the first device/WepPhone client would include an encrypted email address.

More importantly, *Mattaway* explains that the email address is associated with each device through a network address, and that the email address is stored securely on a "connection server" and protected by a firewall server, which insulates the connection server from unauthorized access. *Mattaway* at col.17, ll.44-48; Fig. 15A. In response, Patent Owner asserts the email address could not be the claimed "secure name" because "that email address would already be known to the caller." Response at 20. Patent Owner also asserts that nothing about the "email address" is "associated with any security." Response at 21. Neither point is correct or relevant. Patent Owner attempts to read non-existent limitations into a "secure name" and its representations now are inconsistent with those it made during prosecution when it told the Patent Office this term was not so limited. Indeed, before the Patent Office, the Patent Owner represented that the claimed "secure name" could be as simple as a telephone number, Order at 5, which undoubtedly "would already be known by the caller." Accordingly, *Mattaway* discloses "a first device associated with a secure name and an unsecured name." The Examiner's rejection was proper and should be maintained.

b. *Mattaway Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"*

Patent Owner asserts that *Mattaway* does not satisfy the above requirement because, in one embodiment, there is no message received at the "network address correspondence to the secure name." Response at 21. Patent Owner is wrong. As explained in the Request, the second device retrieves the "network address corresponding to the secure name associated with the first device" from the connection server. Request at 70. The Request also explained that after receiving the IP address of the first device, the second device may "directly establish the point-to-point Internet communications with the [first device] using the IP address of the [first device]." Request at 72. *Mattaway* discloses these "point-to-point Internet communications" are accomplished by the second device "open[ing] up a socket" to the first device. *See Mattaway* at col.24, ll.15-30. The second device transmits a "<CALL>" packet to the first device, to which the first device may, among other things, acknowledge or reject the call. *Mattaway* at col.24, l.11 – col.25, l.12. This process "enables the parties to converse in real-time, telephone quality, <u>encrypted communication</u> over the Internet and other TCP/IP based networks." *Mattaway* at col.25, ll.32-34. Therefore, *Mattaway* discloses this limitation of claim 1, including the requirement of the desire to communicate "securely."

Patent Owner also asserts that a second protocol disclosed in *Mattaway* using a mail server does not satisfy the claim limitations because the "'secure name' (*i.e.*, an email address) is not stored on what the Office and Requester point to as providing security." Response at 21. Patent Owner again is incorrect. The secondary protocol described in *Mattaway* may be used in those situations where the "connection server 26 is non-responsive, unreachable, inoperative, and/or unable to perform the primary point-to-point Internet protocol." *Mattaway* at col.7, ll.54-60. That it may be used as an alternate to the primary protocol does not change the fact that a "secure name" will still be stored on the connection server. Moreover, nothing in the claim requires the "secure name service" to be queried. Thus, *Mattaway* discloses this limitation of claim 1.

c. *Mattaway Discloses "Sending a Message Over a Secure Communication Link from the First Device to the Second Device."*

Patent Owner asserts that *Mattaway* fails to disclose the above limitation because *Mattaway*'s disclosure of "point-to-point Internet communications" and "enable[ing] the parties to converse in real-time, telephone quality, encrypted audio communications" are features located in "disparate portions of *Mattaway*." Response at 22. Patent Owner's assertion is frivolous. The literal distance within the pages of the patent between these two cites is irrelevant—the disclosure of "encrypted communications" in *Mattaway* follows a detailed explanation of the operation of the WepPhone client and is hardly a miscellaneous feature. *See also* Request at 72. Consequently, the Examiner's rejection of Claim 1 was proper and should be maintained.

2. Independent Claim 2

The Examiner correctly found that *Mattaway* discloses every limitation of dependent claim 2. In response, Patent Owner contends that the "connection server" of *Mattaway* does not disclose a "secure name service" because it "does not store a secure name." Response at 22-23. This is incorrect for the same reasons discussed above in section B(1)(a). *See also* Request at 72-74. Patent Owner presents no other distinct response to the rejection of claim 2 based on *Mattaway* relative to its response to the rejection of claim 1. Accordingly, for the reasons noted above, the Examiner's rejection of claim 2 based on *Mattaway* was also proper and should be maintained.

3. Dependent Claims 8, 12, 16-17 and 19-21

Patent Owner presents no distinct response to the rejection of claims 8, 12, 16-17 and 19-21 based on *Mattaway* relative to its response to the rejection of claim 2. Consequently, the Examiner's rejection of these claims based on *Mattaway* was proper and should be maintained. *See also* Request at 75-79.

4. Dependent Claim 7

The Examiner correctly found that *Mattaway* discloses a system "wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed." As the request explains, *Mattaway* shows that the disclosed protocol-based system that includes networked devices that are capable of interacting with "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) on top of the IP." Request at 75. Patent Owner responds only that an additional explanation is needed "to effectuate the claimed feature" and that the protocols identified in *Mattaway* have not "properly been incorporated by reference." Response at 23-24. First, no additional explanation is necessary—the claim only requires that the disclosed system be "capable" of supporting a non-secure communication link. *Mattaway* clearly explains that its devices are accessible through a number of protocols including IP, TCP, RTP and UDP. Request at 75. Such protocols—which were well-known to one skilled in the art—would include those "capable" of supporting such non-secure communication links. Second, it is not necessary that *Beser* incorporate those protocols—all that is necessary is that it explains that the disclosed systems are capable of supporting the protocols, which *Mattaway* has done. Thus, *Mattaway* discloses a system that anticipates claim 7, and the Examiner's rejection was proper and should be maintained.

5. Dependent Claim 9

The Examiner correctly found that *Mattaway* discloses "automatically initiating the secure communication link after it is enabled." In response, Patent Owner argues that *Mattaway* does not disclose the feature of "automatically initiating the secure communication link" as it is silent on that feature. Patent Owner is apparently relying on the putative absence of the terms "automatically initiating" in *Mattaway* to assert that the disclosed initiation of a secure communication link between two WebPhone clients would not occur automatically. As explained in the Request, *Mattaway* describes computer processes that are transparent to the user and thus, within the broadest reasonable scope of the claim term "automatic." Request at 76. As *Mattaway* explains, in response to the return of an "Internet Protocol address of the callee from the global server 1500, the packet transmission sequence illustrated between WebPhones 1536 and 1538 of FIG. 17A transpires." *Mattaway* at col.24, ll.11-14. This step occurs without any interactions by the user that originally made the request. Consequently, the Examiner's rejection of claim 9 was proper.

6. Dependent Claim 13

The Examiner correctly found that *Mattaway* discloses "wherein the receiving and sending of messages through the secure communication link includes multiple sessions." In response, Patent Owner asserts that *Mattaway* cannot disclose this limitation because "each call receives a new session" and Requester has taken the position that a "single call" corresponds to the claimed secure communication link. Patent Owner is incorrect. Request at 76. Initially, Requester did not assert that a "single call" corresponds to the claimed secure communication link. As explained in the Request, the encrypted point-to-point communication link between two WebPhone clients comprises the claimed "secure communication link," not an individual session. Request at 74. And, as *Mattaway* explains that each successive call between a given pair of WebPhone clients would be assigned a "successive session number," *Mattaway* discloses the claimed limitation. Consequently, the rejection of this claim was proper and should be maintained.

7. Dependent Claims 14 and 15

The Examiner correctly found that *Mattaway* discloses every limitation of dependent claims 14 and 15. In response, Patent Owner contends that the requirement of "supporting a plurality of services over the secure communication link" is not met by *Mattaway*. Response at 25. In particular, Patent Owner argues that the "mere recitation of a few alternative names" does not disclose the claimed limitations. *Id.* Patent Owner is incorrect. As the Request explains, *Mattaway* shows that the disclosed protocol-based system that includes networked devices that support "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) on top of the IP." Request at 77. Patent Owner responds only that "additional explanation" is needed "to effectuate the claimed feature" and that the protocols identified in *Mattaway* have not "properly been incorporated by reference." Response at 25. No "additional explanation" is necessary – the claim only specifies "supporting a plurality of services over the secure communication link." Request at 77. *Mattaway* also explains its devices are accessible through a number of protocols including IP, TCP, RTP and UDP. Request at 75. Such protocols—which would be well-known to one skilled in the art—would include those capable of supporting non-secure communication links. Second, it is not necessary that *Beser* incorporate those protocols—all that is necessary is that it explains that the disclosed systems are capable of supporting them, which *Mattaway* has done. Further, as explained in the Request, *Mattaway* also discloses the application program "WEBPHONE® Internet Telephony application," may be utilized for either audio via the UDP protocol or video using UDP and RTP Protocols. Given the breadth of the term "services" as indicated by claim 15, it is clear that *Mattaway* supports a plurality of "services" over the secure communication link. Thus, contrary to Patent Owner's assertion, *Mattaway* discloses a system that anticipates claim 14. Consequently, the Examiner's proposed rejection of claim 14 was proper and should be maintained.

Patent Owner presents no distinct response to the rejection of claim 15 based on *Mattaway* relative to its response to the rejection of claim 14. Accordingly, for the reasons noted above, the Examiner's rejection of claim 15 based on *Mattaway* was also proper and should be maintained.

8. Independent Claim 24

The Examiner correctly found that *Mattaway* describes a method including "at the first device requesting and obtaining registration of a secure name for the first device . . . ." In response, the only new argument presented by Patent Owner is that there is no evidence of "requesting and obtaining registration." Response at 24-25. Patent Owner simply ignores the disclosures in *Mattaway* describing the registration of the secure name at the connection server by a first user upon initiating the "point-to-point Internet protocol." Request at 80. For example, *Mattaway* explains that "in the event that the WebPhone client process is logging on for the first time, global server 1500 returns to the WebPhone 1536 a <USER INFO REQ> packet . . . . In response, WebPhone 1536 returns a <USER INFO> packet" that is used by the connection server to "update database 1516." *Mattaway* at col.22, l.65 – col.23, l.8. A "<REGISTRATION> packet . . . that enables certain functions within the WebPhone" is then transmitted from the global server. *Mattaway* at col.23, ll.5-19. Thus, *Mattaway* plainly shows "requesting and obtaining registration." Patent Owner presents no response to the other limitations in claim 24, but simply relies on assertions made as to other claims. Because the rejections of those other claims were proper, the rejection of claim 24 based on *Mattaway* should be maintained.

9. Dependent Claim 25

In response to the rejection of claim 25, Patent Owner presents no distinct response from those offered for other claims. Because the rejections of those other claims were proper, the rejection of claim 25 based on *Mattaway* should also be maintained. *See also* Request at 83.

10. Independent Claim 26

The Examiner correctly found that *Mattaway* discloses the limitations of claim 26. Patent Owner disagrees, asserting that the storing of the unsecured name in *Mattaway* into the "personal information directory" of the first device does not show the claimed feature of "from the first device requesting and obtaining registration of an unsecured name associated with the first device."

Response at 27-28. Patent Owner's response attempts to read non-existent limitations into the claims – neither the claims nor the specification foreclose the claimed step of "requesting and obtaining registration of an unsecured name" from occurring solely on the first device. In fact, the term "unsecured name" appears nowhere in the specification – Patent Owner's contentions on the implied meaning of this term, thus are made of whole cloth. Because Patent Owner presents no other response to the rejection of claim 26 other than those presented in response to rejections of other claims, and because those other rejections were proper, the rejection of claim 26 based on *Mattaway* was proper and should be maintained.

11. Dependent Claim 27-29

In response to the rejection of claim 27-29, Patent Owner presents no distinct responses from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claims 27-29 based on *Mattaway* were also proper and should be maintained. *See also* Request at 87-93.

C. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3-4, 10-11, 18 and 23 Based on *Mattaway* in view of *Beser* and *RFC 2401* (Issues 4 and 5).

1. Dependent Claims 3 and 4

The Examiner properly found that *Mattaway* in view of *Beser* describes a system that would render claims 3 and 4 obvious to a person of ordinary skill in the art. In response, Patent Owner asserts only that "*Beser* does not make up for the deficiencies noted above regarding *Mattaway's* disclosure." Response at 28-29. Because the Patent Owner presents no distinct response from that offered in response to the rejection of claim 2 based on *Mattaway*, the rejection of claims 3 and 4 was proper and should also be maintained. *See also* Request at 94-95.

2. Dependent Claim 10 and 11

The Examiner correctly found that *Mattaway* in view of *Beser* and *Mattaway* in view of *RFC 2401*discloses each of the limitations of claims 10 and 11. Claim 10 includes the requirement of "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 includes the requirement of "receiving the message in the form of at least one tunneled packet." The Request explains that a person of ordinary skill in the art would have found motivation within *Mattaway* to modify the encrypted communications disclosed therein to incorporate additional mechanisms to add additional layers of protection to the secure communication link. Request at 96-97. That person would have found that each of *Beser* and *RFC 2401* identify the same problem (improving security of networked communications) and provide a solution to that problem; namely, use of a particular type of tunneling. In response, Patent Owner asserts no arguments that are distinct from those already advanced with respect to claims 1 and 2. Accordingly, because the rejection of those claims was proper, the rejection of claims 10 and 11 as obvious was also proper and should be maintained.

3. Dependent Claim 18

The Examiner correctly found that *Mattaway* in view of *Beser* discloses every limitation of dependent claim 18. In response, Patent Owner contends that authentication described in *Beser* has nothing "to do with the alleged secure communication link," and therefore cannot be combined with *Mattaway*. Response at 30. Patent Owner is incorrect. Request at 95-97. The Request explains that the IP 58 packets that comprise the negotiation process "may require encryption and authentication to ensure that the unique identifier cannot be read on the public network." *Beser* at col.11, ll.22-24. As explained above, it is the negotiation process of *Beser*, like *Mattaway*, that facilitates the establishment of the secure communication link. A failure of the authentication described in *Beser* would necessarily preclude the establishment of the secure communication link. Patent Owner's comments thus rest on an assumption that is technically incorrect. Further, as explained in the Request, a person of ordinary skill in the art would have found motivation within *Mattaway* to modify the negotiation process disclosed therein to incorporate additional mechanisms to add another layer of protection to establishing the secure communication link. Request at 97-98. That person would find in *Beser* identification of the same problem (improving security of networked communications) as well as a solution to the same problem, namely, authenticating the secure communication link. Accordingly, the Examiner's rejection of claim 18 was proper and should be maintained.

4. Dependent Claim 23

In response to the rejection of claim 23, Patent Owner presents no distinct response from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claim 23 based on *Mattaway* in view of *Beser* should also be maintained. *See also* Request at 95-97.

D. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-9, 12-15, and 18-29 Based on *Lendenmann* (Issue 6).

1. Independent Claim 1

The Examiner properly found that *Lendenmann* describes a system that anticipates claim 1. In response, Patent Owner asserts *Lendenmann* does not teach a system that discloses (1) "[a] first device associated with a secure name and an unsecured name" or (2) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, (3) "sending a message over a secure communication link from the First Device to the Second Device." Response at 33-35. Each assertion is incorrect.

a. *Lendenmann Discloses "A First Device Associated With A Secure Name and An Unsecured Name"*

Patent Owner asserts that *Lendenmann* does not satisfy the above requirement because the Request "fails to explain how the[] differences" in the disclosed naming schemes "suffice to make X.500 'secure' and DNS 'unsecured.'" Response at 3. Patent Owner simply ignores its own representations before the Patent Office and the literal disclosures of *Lendenmann. See* Request at 102. During prosecution of the '181 patent, the Patent Owner explained that a "secure name" is registered in a "secure name registry" and can include a "secure domain name," but can be as basic as a "telephone number." Order at 5. Further, in a related patent reexamination, the Patent Owner explained that "a conventional domain name service cannot resolve a secure domain name." *Id.* Thus, under its broadest reasonable construction, a "secure name" is defined both by storage in a "secure name registry," and by the fact that it cannot be resolved by a conventional domain name service. A telephone number, according to Patent Owner, would satisfy this definition. Order at 5. Accordingly, as explained in the Request, the CCITT X.500 naming scheme of the DCE environment "is a secure, internal naming convention." Request at 105. The CDS, a directory service component that controls the secure name of a given DCE cell, is integrated into the security server of the CCITT X.500 system and will only complete an operation "if the user is authenticated and authorized." Request at 104. Alternatively, each DCE cell is also represented in the public Internet DNS system with an unsecured name, e.g., a publicly accessible address that may be resolved by a conventional DNS server. Consequently, *Lendenmann* discloses "a first device associated with a secure name and an unsecured name."

b. *Lendenmann Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"*

Patent Owner asserts that *Lendenmann* does not satisfy the above requirement because the Request "does not identify any passage in *Lendenmann* describing receiving any message at a network address corresponding to an X.500 name instead of a DNS name." Response at 35. In particular, Patent Owner contends that *Lendenmann* does not "describe including X.500 addresses in the binding information, much less any security-related consequences of utilizing X.500 names versus DNS names." Patent Owner's arguments are irrelevant to what has been claimed. *See* Request at 106. First, nothing in the claim requires "security-related consequences" to derive from using a "secure name." Moreover, Patent Owner has represented that a "secure name" is defined by where it stored and whether it may resolved by a conventional name server. The CDS of *Lendenmann* is the directory component that controls names and addresses within a DCE Cell. A DCE Cell may have both an X.500 name and a DNS name. Request at 106-07. Second, as explained in the Request, *Lendenmann* explains that "RPC runtime then directly calls the server process listening to the endpoint." Request at 108 (emphasis added). Upon establishment of an "authenticated RPC," the client can "specify the level of protection to be applied to its communication with the server. The protect level determines the degree to which client/server messages are actually encrypted." Request at 108. Thus, *Lendenmann* plainly shows the message from the second device indicating a "desire" to securely communicate with the first device. Accordingly, the Examiner's rejection of claim 1 was proper and should be maintained.

2. Independent Claim 2

The Examiner correctly found that *Lendenmann* discloses every limitation of dependent claim 2. In response, Patent Owner asserts that *Lendenmann* fails to disclose (1) a "'a secure name service'"; (2) "'from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device'"; (3) "'from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device' and 'at the first device, receiving a message containing the network address associated with the secure name of the second device" and (4) "'sending a message to the network address associated with the secure name of the second device using a secure communication link.'" Response at 37-39. Each assertion is incorrect.

a. *Lendenmann Discloses a "Secure Name Service"*

The Request explains that *Lendenmann* describes a "secure name service" in the form of the disclosed Cell Directory Service ("CDS"). Request at 109-115. In response, Patent Owner asserts that "the CDS is not a 'secure name service' because it has no bearing whatsoever on whether the communications for which it provides network addresses are secure or not." Response at 36. Patent Owner's response should be disregarded because it attempts to read non-existent limitations into the term "secure name service."[4] As the Patent Owner has represented to the PTO, a "secure domain name service can resolve addresses for as secure domain name," Order at 5, and a "'secure name' is a name associated with a network address associated [with] a first device" and "can be a secure non-standard domain name" or as basic as "a telephone number." Order at 5. Thus, the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name." Because the X.500 cell naming convention meets these requirements, the CDS is a "secure name service."

b. *Lendenmann* Discloses a "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device'"

The Request explains how *Lendenmann* discloses the above limitation. Request at 109. In rebuttal, Patent Owner contends that *Lendenmann* does not describe "requesting a network address associated with any server name at all, let alone a secure name." Response at 37. Patent Owner is incorrect. In fact, Patent Owner admits that "*Lendenmann* generically describes that its CDS may return a network address upon receiving a name." Response 37. But, more than "generically describing" the CDS, *Lendenmann* explains, exactly as specified in the claims, that "[t]he CDS stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource." Request at 113. That the CDS may perform in addition other functions is irrelevant to whether it meets this particular claim requirement.

c. *Lendenmann* Discloses a "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device' and 'at the first device, receiving a message containing the network address associated with the secure name of the second device"

As explained in the Request, *Lendenmann* discloses the above limitation. Patent Owner does not substantively contest this point — other than repeating its earlier arguments. Instead,

[4] Patent Owner's contention that *Lendenmann* does not disclose a "secure name" is also incorrect for reasons provided above with respect to claim 1.

Patent Owner asserts that, under *NetMoneyIN, Inc. v. Verisign, Inc.*, 545 F.3d 1359 (Fed. Cir. 2008), Requester improperly "pick[s] and choos[es]" various features of *Lendenmann* to show the contested claims are unpatentable. Patent Owner's reliance on *NetMoneyIN* is misplaced. *NetMondyIN* simply held that the particular reference at issue in that case would not have been read as the defendant had proposed. By contrast, no third party interpretation of *Lendenmann* is needed here – it expressly discloses the features required by the claims via its description of the DCE system—including "requesting a network address associated with the secure name" and "receiving a message containing the network address associated with the secure name. Request at 111-114. Moreover, that these features may be optionally implemented within the DCE system does not mean *Lendenmann* does not disclose a system that comprises those features.

d. *Lendenmann* Discloses a "Sending a Message to the Network Address Associated With the Secure Name of the Second Device Using a Secure Communication Link."

The Request explains that *Lendenmann* describes "sending a message to the network address associated with the secure name of the second device using a secure communication link." Patent Owner responds that the "secure communication link" of *Lendenmann* does not have "anything to do with the allegedly secure (X.500) or unsecured (DNS) names." Response at 39. Patent Owners employs a fundamentally implausible reading of *Lendenmann* – that it "its RPC-related security features … [do not] … have anything to do with the allegedly secure (X.500) … names." In other words, Patent Owner contends that the secure names in Lendenmann have nothing to do with the mechanisms that ensure secure communications to destinations associatd with those names. Obviously, Patent Owner is incorrect. Moreover, Patent Owner again attempts to read non-existent limitations into the claims. In reality, *Lendenmann* discloses exactly what the claims require: "sending a message to the network address associated with the secure name of the second device using a secure communication link." Request at 114-115. The Examiner's rejection of this claim was based on a correct reading of *Lendenmann* and the claims, and should be maintained.

3. Dependent Claims 3-4, 12-15, 18-20, and 22-23

Patent Owner presents no distinct response to the rejection of claims 3-4, 12-15, 18-20, and 22-23 based on *Lendenmann* relative to its response to the rejection of claim 2 over *Lendenmann*. Consequently, for the reasons noted above, the Examiner's rejection of claim 3-4, 12-15, 18-20, and 22-23 based on *Lendenmann* was proper and should be maintained. *See also* Request at 115-

117, 123-126.

4. Dependent Claims 5 and 6

The Examiner correctly found that *Lendenmann* anticipates every limitation of dependent claims 5 and 6. Patent Owner responds that the *Lendenmann* does not include "receiving a message in encrypted form," or "decrypting the message" (claim 6). As it does repeatedly, Patent Owner's response is limited to the charge that the Request "cobbles together short excerpts from throughout *Lendenmann* without regard to whether they reflect the actual role that *Lendenmann* describes for the CDS in establishing RPCs." Patent Owner is incorrect, as it simply ignores the disclosures in *Lendenmann* that expressly describe the CDS's implementation into the "security service" of the DCE and the use of RPC routines in order to query the CDS. Request at 117-119. Further, as already demonstrated above, clients can establish a level of protection with an established RPC that "determines the degree to which client/server messages are actually encrypted." Request at 119. Accordingly, the Examiner's rejection of claims 5 and 6 was proper.

5. Dependent Claim 21

The Examiner properly found that *Lendenmann* describes a system that would render claim 21 invalid. In response, Patent Owner asserts that "*Lendenmann* does not disclose any secure or unsecure names," and furthermore, that the CDS does not provide "both a network address corresponding to an X.500 name (an allegedly secure name) *and a DNS name itself* (an alleged unsecured name) to the claimed "first device." Response at 41 (emphasis in original). Patent Owner is incorrect. Request at 127. First, as demonstrated above and as Patent Owner effectively admits, *Lendenmann* does disclose both secure and unsecure names. Second, *Lendenmann* discloses both a secure name and unsecured name for a given cell. As explained in the Request, DCE makes use of both X.500 naming scheme and DNS, a global addressing and routing scheme that describes unsecured names. Request at 127. The Request also explains that the DCE system includes a function called "cell-name aliasing" which permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name," such as a primary X.500 name and DNS name as the cell alias. Request at 111-12. Accordingly, the Examiner's rejection of this claim was proper and should be maintained.

6. Independent Claim 24 and Dependent Claim 25.

The Examiner correctly found that *Lendenmann* describes each and every limitation of claims 24 and 25. In response, Patent Owner asserts that Requester has "change[d] their position by asserting that *all* names stored within the CDS are "secure," whether X.500 or DNS." Response at 41. Patent Owner is incorrect – neither the Office nor the Requester contended that *Lendenmann* shows that "all names stored in a CDS are secure." Patent Owner's assertions are also entirely irrelevant to the claims, which make no mention of use of "unsecured" names. Apart from these incorrect and irrelevant assertions, Patent Owner presents no response substantively different from its response to claims 1 and 2. Because the rejections of those claims were proper, the rejection of claims 24 and 25 is also proper and should be maintained.

7. Independent Claim 26 and Dependent Claim 27.

The Examiner correctly found that *Lendenmann* describes each and every limitation of claims 26 and 27. In response, Patent Owner asserts that *Lendenmann* does not disclose that a server may be registered with an "additional 'unique network address.'" Response at 42. Patent Owner is incorrect. As explained in the Request, the DCE system permits devices anywhere in the DCE system to obtain the network address of any other advice to engage in communications. Request at 141. The X.500 naming convention requires each device to be discoverable using both its unsecured name (e.g., the domain name) and its secure name (e.g., the X.500 secure identifier). The X.500 and domain names associated with a device in the *Lendenmann* scheme thus comprise both a unsecure and a unique secure network address. As Patent Owner present no other response to these claims, and the rejection of those claims was proper, the rejection of claims 26 and 27 was proper and should be maintained.

8. Independent Claim 28

In response to the rejection of claim 28, Patent Owner presents no distinct response from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claim 28 based on *Lendenmann* should also be maintained. *See also* Request at 147-153.

9. Independent Claim 29

In response to the rejection of claim 29, Patent Owner presents no distinct response from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claim 29 based on *Lendenmann* should also be maintained. *See also* Request at 153-160.

E. Response to Patent Owner's Arguments Regarding the Rejection of Claims 10, 11 and 17 Based on *Lendenmann* in view of *Beser* (Issue 7).

The Examiner properly found that *Lendenmann* in view of *Beser* describes a system that would render obvious claims 10, 11 and 17. In response, Patent Owner asserts only that *Beser* does not remedy the deficiencies of *Lendenmann.* Response at 43. Because the Patent Owner presents no distinct response from that offered in response to the rejection of claim 2 based on *Lendenmann*, the rejection of claims 10, 11, and 17 was proper and should also be maintained. *See also* Request at 161-163, 164.

F. Response to Patent Owner's Arguments Regarding the Rejection of Claims 10 and 11 Based on *Lendenmann* in view of *RFC 2401* (Issue 8).

The Examiner properly found that *Lendenmann* in view of *RFC 2401* describes a system that would render obvious claims 10 and 11. In response, Patent Owner asserts only that *RFC 2401* does not remedy the deficiencies of *Lendenmann.* Response at 43. Because the Patent Owner presents no distinct response from that offered in response to the rejection of claim 2 based on *Lendenmann*, the rejection of claims 10 and 11 was proper and should also be maintained. *See also* Request at 164-166.

G. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-23 and 28-29 Based on *Provino* (Issue 9).

1. Independent Claim 1

The Examiner properly found that *Provino* describes a system that anticipates claim 1. In response, Patent Owner asserts *Provino* does not teach a system that discloses (1) "a first device associated with a secure name and an unsecured name," (2) "a 'secure name'" (3) "a first device" and (4) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." Response at 46. Each of these is incorrect.

a. *Provino Discloses "A First Device Associated With a Secure Name and Unsecured Name"*

The Examiner correctly found that *Provino* discloses "a first device associated with a secure name and unsecured name." In response, Patent Owner asserts that *Provino* does not satisfy the above requirement because the Request is "flawed, as *Provino's* system does not function the way Requestor alleges." Response at 45. Patent Owner is incorrect. As explained in the Request, *Provino* discloses two name servers, Name Server 17 and VPN Name Server 32. Request at 168. *Provino* also discloses two names are associated with servers on Virtual Private Network 15. The first, a secure name, is the domain name associated with a given VPN server (item 31(S), for example), stored in the VPN Name Server 32. The second, an unsecure name, is the domain name of firewall 30, which is also associated with each of the VPN servers (item 31(s), for example). Request at 168; *see also* Fig. 1. Thus, Provino plainly does show a first device associated with a secure name and an unsecure name. Patent Owner's contention that the Request "has not identified any device in *Provino* that is associated with both a "secure name" and an "unsecured name" is, thus, both wrong and improperly reads non-existent limitations into the term "associated." As the claims are not so limited, the rejection as imposed was proper and should be maintained.

b. *Provino Discloses a "Secure Name"*

The Examiner correctly found that *Provino* discloses a "secure name." In rebuttal, Patent Owner contends that *Provino* does not disclose a "secure name" because its name servers "are conventional name servers of the type distinguished in the '181 patent specification and do not qualify as a 'secure name service' that can resolve 'secure names.'" Response at 45. Patent Owner's analysis is both irrelevant and incorrect. First, the only "secure name service" identified in the Request is VPN Name Server 32; Patent Owner's analysis of Name Server 17 here is irrelevant. Request at 168. Second, the role of VPN Name Server 32, as explained in the Request, is no different than the definition Patent Owner provides in its response: "a service that both resolves a name into a network address and further supports establishing a secure communication link." Response at 45. Indeed, the Request explains that VPN Name Server 32 "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses. Request at 168. Further, VPN Name Server 32 is not accessible in the same manner as a conventional domain name service. As described in the Request, the secure communication link with the second device is facilitated by VPN Name Server 32, which only provides an authorized device with the second device's secure name. Request at 169. For the above reasons, this requirement is disclosed by *Provino.*

c. *Provino Discloses the Claimed "First Device."*

The Examiner correctly found that *Provino* discloses the claimed "first device." Claim 1 specifies simply "receiving, at a network address corresponding to the secure name *associated with the first device*, a message from a second device of the desire to securely communicate with the first device." Provino unquestionably shows this - the Request explains that *Provino* shows device 12(m), identified repeatedly above as the claimed "second device," sends "a message packet for transfer from the ISP 11 and Internet 14 to the *firewall 30* requesting establishment of a secure tunnel between the device 12(m) and firewall 30." Request at 171. Rather than respond substantively to this, Patent Owner asserts the Request "mixes and matches features from different devices in its attempt to show unpatentability." Response at 45-46. Patent Owner's assertion is irrelevant, as it simply ignores the actual disclosure of *Provino.*

d. *Provino Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"*

Patent Owner presents no distinct response to the explanation in the Request that the above limitation is described by *Provino*, other than to repeat its assertions regarding the other limitations discussed above. As those assertions are incorrect, the rejection of claim 1 based on *Provino* was proper and should be maintained. *See also* Request at 168.

2. Independent Claim 2

In response to the rejection of claim 2, Patent Owner presents no distinct response relative to those offered for claim 1. Because the rejection of claim 1 was proper, the rejection of claim 2 based on *Provino* should also be maintained. *See also* Request at 172-176.

3. Claims 3-15, 18-23, and 28-29

Patent Owner presents no distinct response to the rejection of claims 3-15, 18-23 and 28-29 based on *Provino* relative to its response to the rejection of claim 1 based on *Provino*. Because the rejection of that claim was proper, the Examiner's rejection of claims 3-15, 18-23 and 28-29 based on *Provino* was proper and should be maintained. *See also* Request at 176-188.

H. Response to Patent Owner's Arguments Regarding the Rejection of Claims 24-26 Based on *Provino* in *H.323* (Issue 10).

1. Independent Claim 24 and Dependent Claim 25

The Examiner correctly found that *Provino* in view of *H.323* renders obvious claims 24 and 25. In response, Patent Owner presents no response distinct from that offered to the rejection of claim 1 over *Provino* or *H.323*. Because that rejection was proper, the rejection of claims 24 and 25 based on *Provino* in view of *H.323* was also proper and should be maintained. *See also* Request at 188-193.

2. Independent Claim 26

The Examiner correctly found that *Provino* in view of *H.323* renders obvious claim 26. In response, Patent Owner asserts that *H.235* is not "incorporated by reference into *H.323* and is therefore not properly considered to be part of that document." Response at 50. Patent Owner is incorrect. As explained in the request, *H.323* expressly incorporates *H.235* as "constituting provisions of this [i.e., the *H.323*] Recommendation." Request at 204 (citing *H.323* at 2-3). Accordingly, Patent Owner's "procedural" argument is wrong. Further, Patent Owner's so-called "substantive []" arguments with respect to these claims present no distinct response from that offered in claim 1. Because the rejection of claim 1 was proper, the rejection of claim 26 based on *Provino* in view of *H.323* was also proper and should be maintained.

I. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-29 Based on *H.323* (Issue 11).

1. Independent Claim 1

The Examiner properly found that *H.323* describes a system that anticipates claim 1. In response, Patent Owner asserts that (1) "[c]ombining the teachings of *H.323, H.245, H.235*, and *H.225* is improper," (2) *H.323* does not disclose "[a] first device associated with a secure name and an unsecured name," (3) *H.323* does not disclose "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, and (4) "sending a message over a secure communication link from the First Device to the Second Device." Response at 51-59. Each of these is incorrect.

a. *The Teachings of H.323, H.245, H.235, and H.225 Are Properly Combined*

The Examiner correctly found that the above-cited H-series recommendations are expressly incorporated as part of the disclosure of *H.323*, which anticipates claim 1. In response, Patent Owner asserts that *H.323* does not properly incorporate the teachings of *H.323, H.245, H.235,* and *H.225* because *H.323* "does not identify with detailed particularity the subject matter" of those references. Response at 52. Patent Owner is incorrect. First, as explained in the request, *H.323* expressly incorporates *H.245, H.235,* and *H.245* as "constituting provisions of this [i.e., the *H.323*] Recommendation." Request at 204 (citing *H.323* at 2-3). That is sufficient. *See Harari v. Lee*, 656 F.3d 1331, 1335 (Fed. Cir. 2011)(holding "broad and unequivocal" language sufficient to incorporate the entire disclosure of another reference). Even under the previous standard cited by Patent Owner, each of *H.245, H.235*, and *H.245* was properly incorporated by reference into *H.323*. For example, *H.323* explains that "authentication and security for H.323 is optional; however, if it is provided, <u>it shall be provided in accordance with Recommendation H.235</u>." *H.323* at 81 (emphasis added). Similarly, *H.323* discloses that products claiming compliance with

Version 2 of H.323 shall comply with all of the mandatory requirements of H.323 (1998) which references Recommendations H.225[] (1998) and H.245 (1998)." *H.323* at (i) (emphasis added). *H.323* also describes *H.225* as containing "[c]all signaling protocols and media stream packetization for packet based multimedia communication systems," and *H.245* as containing "[c]ontrol protocol for multimedia communication." *H.323* at 2-3. *H.323* thus clearly incorporates by reference the teachings of *H.225, H.235,* and *H.245*. Accordingly, the Examiner's rejection of this claim was proper and should be maintained.

b. *H.323 Discloses "A First Device Associated With A Secure Name and An Unsecured Name"*

The Examiner correctly found that *H.323* discloses the above limitation. In rebuttal, Patent Owner contends that *H.323* does not describe a "first device associated" with both "a secure name and unsecured name." Response at 54. Patent Owner is incorrect. As explained in the Request, *H.323* discloses that each device in an H.323 network "is associated with one or more alias names, called Alias addresses, which can be in the form of a phone number or an email address." Request at 204. Alias addresses are "secure," in part, because they are "protected by 'access tokens,' which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses." Request at 204. Further, the Requester notes again that during prosecution of the '181 patent, for example, the Patent Owner explained that a "secure name" is registered in a "secure name registry" and can include a "secure domain name," but can be as basic as a "telephone number." Order at 5. And, in a related patent reexamination, the Patent Owner explained that "a conventional domain name service cannot resolve a secure domain name." *Id.* Thus, under the broadest reasonable construction, a "secure name" is defined both by storage in a "secure name registry," and because it cannot be resolved by a conventional domain name service. According to Patent Owner, a telephone number, such as the "alias address" described in *H.323*, would satisfy this construction.

Moreover, secure names, the Request explains, are registered with a "Gatekeeper" in addition to "be[ing] associated with the unsecured names of the Gatekeeper computer with which they are registered." Request at 210. In response, Patent Owner contends that the Request has not identified any device in *H.323* that is associated with both a "secure name" and an "unsecured name." Response at 45. Patent Owner's response attempts to read non-existent limitations into the term "associated" – the plain language of this term refutes Patent Owner's assertions.

c. *H.323 Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message*

From a Second Device of the Desire[] to Securely Communicate With the First Device"

The Examiner correctly found that *H.323* discloses the above claim requirement. In response, Patent Owner asserts a number of new, implausible arguments. First, Patent Owner contends that *H.323* "does not describe receiving any message at a network address corresponding to an access-token-protected alias *rather than* a second, allegedly 'unsecured'alias." Response at 56. Patent Owner ignores the Request and the *H.323* disclosure, which clearly explain that one endpoint receives a request from another endpoint of the desire to communicate securely, and that these endpoint may further be protected by "access tokens," which are utilized to "obscure or hide destination addressing information." Request at 213-17. As for Patent Owner's statement that "as explained above with respect to *Beser*, merely shielding the endpoints of communications does 'not secure those communications from eavesdropping'"—the Examiner has already found that statement to be irrelevant, as described above. *See also* ACP at 32-22 ("Encryption is more secure than hiding the source address just as encryption and hiding the address is more secure than encryption only. The claims however do not recite the degree of security.")

Patent Owner next asserts that the "IPsec passage of *H.235* also fails to support the rejection." In particular, Patent Owner contends "the only address disclosed in this passage corresponds to a 'call signaling channel,' not to an endpoint (*i.e.*, an alleged "first device")." Response at 57. Patent Owner is mistaken. As explained in the Request, the second device, i.e., "the calling endpoint," together with its "gatekeeper," would establish a "call signaling channel" by retrieving and communicating the "address and port number of the call signaling channel in the called endpoint." Request at 215. After establishing the "call signaling channel" (which is used to carry call control messages), the "endpoints can negotiate the use of IPSEC for the H.245 channel" on the "Q.931 SETUP and CONNECT exchange." Request at 216. During the Q.931 SETUP and CONNECT exchange process, the Gatekeepers will facilitate, for example, "routed call signaling." H.323 at Fig.23 at 51-52 ("Endpoint 1 (calling endpoint) initiates the ARQ (1)/ACF (2) exchange with Gatekeeper 1. Gatekeeper 1 shall return a Call Signaling Channel Transport Address of itself in the ACF (2). Endpoint 1 then sends the Setup (3) message using that Transport Address. Gatekeeper 1 then sends the Setup (4) message to the well-known Call Signaling Channel Transport Address of Endpoint 2. If Endpoint 2 wishes to accept the call, it initiates the ARQ (6)/ACF (7) exchange with Gatekeeper 2.2."). Patent Owner's argument that the communication in *H.323* "occurs only *after* security features have been employed" is also incorrect. The Request explains that the endpoints negotiate the user of IPSEC during the setup process. Request at 216.

Patent Owner next contends that the "call control (H.245) security" and "media stream privacy" do not support the rejection because "these passages do not describe receiving any message at a network address corresponding to an access token or an access-token protected alias address." Response at 58. Patent Owner is incorrect for the reasons stated above. Further, Patent Owner seems to contend that it is significant that certain security features may be within the discretion of the calling endpoint. Response at 58. Patent Owner's assertion is irrelevant, as the fact that the calling endpoint may choose to implement IPSEC is exactly what the anticipated claim calls for, i.e., "a message from a second device of the desire to securely communicate with the first device." Accordingly, the Examiner was correct to find that *H.323* discloses this limitation.

d. *H.323* Discloses "Sending a Message over a Secure Communication Link from the First Device to the Second Device."

The Examiner correctly found that *H.323* discloses the above claim requirement. In response, Patent Owner raises no arguments that are distinct from its other arguments related to claim 1. Because the Examiner was also correct to find that *H.323* discloses those requirements above, the rejection of this claim was proper and should be maintained. *See also* Request at 217.

2. Independent Claim 2

The Examiner correctly found that *H.323* discloses every limitation of dependent claim 2. In response, Patent Owner alleges that *H.323* fails to disclose (1) "a secure name"; (2) "a network address associated with the secure name of the second device"; (3) "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device' and 'at the first device, receiving a message containing the network address associated with the secure name of the second device" and (4) "'from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.'" Response at 37-39. Each of these is incorrect.

a. *H.323 Discloses "A Secure Name"*

The Examiner correctly found that *H.323* discloses "a secure name." In rebuttal, Patent Owner presents no arguments that are distinct from those already presented with respect to claim 1. Accordingly, for the reasons demonstrated above, the Examiner's finding was correct. *See also* Request at 218-226.

b. *H.323* Discloses "A Network Address Associated with the Secure Name of the Second Device"

The Examiner correctly found that *H.323* discloses every limitation of claim 1. In response, Patent Owner presents no arguments that are distinct from those already presented with respect to claim 1. As explained in the Request and above, after establishing the "call signaling channel" (which is used to carry call control messages), the "endpoints can negotiate the use of IPSEC for the <u>H.245 channel</u>" on the "Q.931 SETUP and CONNECT exchange." Request at 216. In turn, during the Q.931 SETUP and CONNECT exchange process, for example, the Gatekeepers will facilitate "routed call signaling." H.323 at Fig.23 at 51-52 ("Endpoint 1 (calling endpoint) initiates the ARQ (1)/ACF (2) exchange with Gatekeeper 1. Gatekeeper 1 shall return a Call Signalling Channel Transport Address of itself in the ACF (2). Endpoint 1 then sends the Setup (3) message using that Transport Address. Gatekeeper 1 then sends the Setup (4) message to the well-known Call Signalling Channel Transport Address of Endpoint 2. If Endpoint 2 wishes to accept the call, it initiates the ARQ (6)/ACF (7) exchange with Gatekeeper 2.2."). Accordingly, the Examiner's finding that H.323 discloses this element was correct.

c. *H.323* Discloses a "From the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated With the Secure Name of the Second Device' and 'at the First Device, Receiving a Message Containing the Network Address Associated With the Secure Name of the Second Device"

The Examiner correctly found that *H.323* discloses the above claim requirement. Patent Owner responds that the disclosed access tokens "provide privacy by shielding an endpoint's Transport Address and Alias Address information from a calling party" and therefore necessarily prevent the calling endpoint from receiving the network address, which Patent Owner contends is required by this element of claim 2. Patent Owner is incorrect. First, the disclosed "access tokens" are an <u>additional</u> feature of the *H.323* system that contribute an <u>additional</u> element of security to the disclosed point-to-point communications. Request at 219-21. So, while an "access token" may be sufficient to render an "alias address" a secure name, "access tokens" are not necessary. Patent Owner's remaining arguments with respect to this limitation hinge on this incorrect assumption. Response at 60-62. As explained above, Patent Owner has represented that a "secure name" can, like the "alias addresses" of *H.323*, be as basic as a telephone number. Second, even assuming that the "alias addresses" required the "access token" feature to be considered "secure names," *H.323* satisfies the above claim requirement nonetheless. As explained in the Request, "calls using the Access Token can be routed through the Gatekeeper to the called endpoint." Request at 220. In such situations, the Access Token identifies the Gatekeeper, and particularly the address of the Gatekeeper in order to communicate with a given endpoint. Patent Owner next contends that "a calling endpoint using an access token never receives a network address associated with the access-token-protected alias address." Response at 60. Yet, the claims impose no such requirement, and Patent Owner's response which presumes this to be the case should be disregarded, as it attempts to read non-existent limitations into the term "associated."

Patent Owner's remaining arguments present no issues distinct from those presented with respect to the other requirements of claims 1 and 2, or simply misunderstand the Request. Accordingly, the Examiner's rejection of claim 2 was proper and should be maintained.

d. *H.323 Discloses "From the First Device, Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"*

The Examiner correctly found that *H.323* discloses the above claim requirement. In response, Patent Owner presents no arguments that are distinct from those already presented with respect to the other requirements of claims 1 and 2. Those arguments have been fully addressed above, and consequently, the rejection of claim 2 was proper and should be maintained. *See also* Request at 224.

3. Claims 3, 6-7, 12, 14-20, 22 and 23

Patent Owner presents no distinct response to the rejection of claims 3, 6-7, 12, 14-20, 22 and 23 based on *H.323* relative to its response to the rejection of claims 1 and 2 based on *H.323*. Consequently, because the rejection of those claims was proper, the Examiner's rejection of claims 3, 6-7, 12, 14-20, 22 and 23 based on *H.323* was proper and should be maintained. *See also* Request at 226-227, 228-229, 231-232, 233-237, 241-242.

4. Dependent Claim 4

The Examiner correctly found that *H.323* anticipates every limitation of dependent claim 5. Patent Owner responds that the Request "improperly mixed and matched various distinct components of various different references in attempting to meet the claim language." Response at 63. Patent Owner is incorrect. As explained the Request and above, *H.323* expressly incorporates by reference each of the H-series recommendations, including *H.235*. Further, the Request demonstrates that these endpoints may further be protected by "access tokens," which are utilized to "obscure or hide destination addressing information." Request at 220. The access tokens, which obfuscate the destination address information, thus "indicate security." *See also* ACP at 32-32 ("Encryption is more secure than hiding the source address just as encryption and hiding the address is more secure than encryption only. The claims however do not recite the degree of security.") Consequently, the Examiner's rejection of claim 4 was proper.

5. Dependent Claim 5

The Examiner correctly found that *H.323* anticipates every limitation of dependent claim 5. Patent Owner presents no response distinct from its response to the rejection of claim 2. Accordingly, because the rejection of those claims was proper, the Examiner's rejection of claim 2 based on *H.323* was proper and should be maintained.

6. Dependent Claims 9

The Examiner correctly found that *H.323* anticipates dependent claim 9. Patent Owner is apparently relying on the literal absence of the words "automatically initiating" in *H.323* to assert that the disclosed initiation of a secure communication link established upon completion of negotiation process between networked devices would not occur automatically. As explained throughout the Request, *H.323* describes processes that would be both automatic and transparent to the user. For example, *H.323* explains that "[a]fter obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair." Request at 219. These steps occur without any interaction from the endpoint that originally made the request to engage in secure communications. Accordingly, the rejection of claim 9 was proper.

7. Dependent Claim 10 and 11

The Examiner correctly found that *H.323* discloses each of the limitations of claims 10 and 11. Claim 10 includes the requirement of "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 includes the requirement of "receiving the message in the form of at least one tunneled packet." As the Office Action explains, each of these claims are additionally satisfied by *H.323's* disclosure of an "encapsulation" or "tunneling technique" as described in *H.245*. In response, Patent Owner contends that the "Request only discloses an address corresponding to a 'call signaling channel'—not an endpoint (*i.e.,* alleged "second device")." Patent Owner is incorrect for the reasons explained above.

Further, the Office Action explains that "*when tunneling is active, one or more H.245 messages can be encapsulated in any Q.931 message*." OA at 12. Encapsulating a Q.931 message, of course, would include "Q.931 SETUP" messages, which involve the negotiation and establishment of the secure communication link. Accordingly, the Examiner's rejection of these claims was proper and should be maintained. *See also* Request at 230-231.

8. Dependent Claim 13

The Examiner correctly found that *H.323* discloses every limitation of claim 13, which specifies that the "receiving and sending of messages through the secure communication link includes multiple sessions." As explained in the Request, *H.323* employs "multiple logical channels and RTP sessions" over a secure communication link. Request at 232-233. In response, Patent Owner contends that *H.*323 does not disclose this requirement because the H.323 layering technique "should employ a separate channel and separate session." Response at 64. As Patent Owner's comment acknowledges, this manner of implementation is option to the H.323 processes. Response at 65. Patent Owner's response also reads non-existent limitations into the term "secure communication link." As the claims are not so limited, the rejection as imposed was proper and should be maintained.

9. Dependent Claim 21

The Examiner correctly found that *H.323* anticipates every limitation of dependent claim 21. Patent Owner presents no response distinct from its response to the rejection of claim 1. Accordingly, because the rejection of claim 1 was proper, the Examiner's rejection of claim 21 based on *H.323* was proper and should be maintained. *See also* Request at 237-241.

10. Independent Claim 24 and Dependent Claim 25

The Examiner correctly found that *H.323* anticipates every limitation of claims 24 and 25. Patent Owner presents no response distinct to its response to the rejection of claims 1 and 2. Accordingly, because the rejection of those clams was proper, the Examiner's rejection of claims 24 and 25 based on *H.323* was proper and should be maintained. *See also* Request at 242-248.

11. Independent Claim 26 and Dependent Claim 27

The Examiner correctly found that *H.323* anticipates every limitation of claims 26 and 27. Patent Owner presents no response distinct from its response to the rejection of claims 1 and 2. Accordingly, because the rejection of those clams was proper, the Examiner's rejection of claims 26 and 27 based on *H.323* was proper and should be maintained. *See also* Request at 248-257.

12. Independent Claim 28

The Examiner correctly found that *H.323* anticipates every limitation of claim 28. Patent Owner presents no response to claim 28 distinct from its response to the rejection of claims 1 and 2. Accordingly, because the rejection of claims 1 and 2 was proper, the Examiner's rejection of claims claim 28 based on *H.323* was proper and should be maintained. *See also* Request at 258-263.

13. Independent Claim 29

The Examiner correctly found that *H.323* anticipates every limitation of claim 29. Patent Owner presents no response to claim 29 distinct from its response to the rejection of claims 1 and 2. Accordingly, because the rejection of those clams was proper, the Examiner's rejection of claims claim 29 based on *H.323* was proper and should be maintained. *See also* Request at 263-268.

J. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-29 Based on *Johnson* in view of *RFC 2131, RFC 1034,* and *RFC 2401* (Issue 13).

1. Independent Claim 1

The Examiner properly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claim 1. In response, Patent Owner asserts *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* do not teach a system that discloses (1) "a first device associated with a secure name and an unsecured name"; (2) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device," and (3) "sending a message over a secure communication link from the first device of the second device." Response at 67-70. Each of these is incorrect.

a. *Johnson in view of RFC 2131, RFC 1034 and RFC 2401 Discloses a "First Device Associated With a Secure Name and an Unsecured Name"*

Patent Owner first asserts that *Johnson* "does not disclose any secure names." Response at 68. Patent Owner is incorrect. As explained in the Request, a name registered by the secure name server constitutes a "secure name" because, for example, it requires authorization to access and is protected through encryption." Request at 272. Further, as the Office observed, Patent Owner made representations during prosecution of the related '180 patent about the meaning of the terms "secure name" and "secure name service" that were different than its present assertions. Office Action at 5. Specifically, Patent Owner stated that a "*'secure name' is a name associated with a* *network address associated of a [SIC] first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device.*" Order at 5 (emphasis added). The Secure Name Server 14 disclosed in *Johnson* at least satisfies this broad construction. Patent Owner's claim that Secure Name Server 14 "is a conventional name server" is also simply incorrect. As described in the Request, the secure communication link with the second device is facilitated by Secure Name Server 14, which only provides a network address associated with a secure name to an authorized requesting device. Request at 272-75. A conventional name server would not have such security features in place. Finally, Patent Owner's argument that secure name server 14 does not provide "any further support for establishing a secure communication link" is baseless. Indeed, nothing in the claim or in Patent Owner's representations to the Patent Office requires that a secure name service "provide any further support for establishing a secure communication link." Patent Owner again attempts to improperly read non-existent limitations into claim 1.

Patent Owner next asserts that the Request does not demonstrate that "*Johnson* discloses or suggests a 'secure name' even under their [Requester's] own interpretation of that term." Response at 68. Patent Owner's analysis is incorrect and irrelevant. First, as demonstrated above, the Request shows that *Johnson* discloses a "secure name" under Patent Owner's own interpretation of that term. Second, Patent Owner next contention – "the user accessing the secure name server 14 must presumably already know the name of the secure mail server before the alleged authorization and encryption" – again tries to read non-existent limitations into the claims. Response at 68. Nothing in specification or claims requires that a secure name not be "known" in advance of a request to access that name.

Patent Owner also contends that the Request "incorrectly allege[s] that the claimed 'unsecured name' is disclosed by a domain name of the secure name server 14 . . . ." The Request explained that *Johnson* shows two alternatives, one where the client identifier for secure name server 114 is an unsecured name, and the other where the secure server's name itself is used. The Request also explained that where the secure server name is used to conduct transactions over the Internet, that would be done consistent with established Internet standards (e.g., RFC 1034). See Request at 273-274. The Request explained in that embodiment, it would be known to use a registered domain name, as that was commonplace at the time. *Id.* Patent Owner's convoluted hypothetical at page 69 of the Response, thus, ignores the actual claim language and severely mischaracterizes the Request. Patent Owner also contests the description of *Johnson*, asserting that it does not indicate "the secure mail server has a domain name registered in the public DNS system and/or a client identifier associated with such domain that constitutes an 'unsecured name.'" The Request at 273-274 reproduced excerpts from Johnson and explained why this description, contrary to Patent Owner's assertions, is correct. Moreover, Patent Owner has not explained how this particular detail is relevant to the claim 1. In reality it is not.

b. *Johnson in view of RFC 2131, RFC 1034 and RFC 2401 Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"*

Patent Owner asserts that *Johnson* does not describe systems showing this element because *Johnson* "does not disclose or suggest a 'secure name,'" relying on its arguments above. But, as already demonstrated, Patent Owner is incorrect. Patent Owner also contends that the references "are lacking regarding the 'message from a second device of the desire[] to securely communicate with the first device." Patent Owner's analysis is simply wrong. As explained in the Request, the "first user 12" utilizes the prescribed authentication procedures and the network address of the secure mail server 16 in order to send an "electronic mail message [] protected by a protection method, such as encryption . . . to the designated recipient's box on the secure electronic mail server 16." Request at 275. Accordingly, *Johnson* describes this element of claim 1.

c. *Johnson Discloses "Sending a Message Over a Secure Communication Link from the First Device to the Second Device."*

The examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious a system that includes the above requirement. In response, Patent Owner asserts, remarkably, that *Johnson* does not disclose this limitation because the first and second devices are "reversed." Response at 70. In other words, Patent Owner contends that *Johnson* should be read to suggest only one-way communications. This is an obviously implausible reading of *Johnson.* Plainly, the so-called "first device" of *Johnson* may function as a "second device" depending upon which device in *Johnson* initiates the secure communication. Accordingly, the Examiner's rejection of the claim was proper and should be maintained. *See also* Request at 270-276.

2. Independent Claim 2

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* discloses every limitation of dependent claim 2. Patent Owner presents no response distinct from its response relative to its assertions for claim 1. Because the rejection of claim 1 was proper, the Examiner's rejection of claim 2 was also proper and should be maintained. *See also* Request at 276-282.

3. Dependent Claims 4-6, 8, 12 and 17-20

Patent Owner presents no response distinct from its response to the rejection of claims 4-6, 8, 12 and 17-20 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* relative to its response to the rejection of claim 2. Consequently, because the rejection of those claims was proper, the Examiner's rejection of claims 4-6, 8, 12 and 17-20 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained. *See also* Request at 284-286, 287-289, 291-292, 294-297.

4. Dependent Claim 3

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered dependent claim 2 obvious to a person of ordinary skill in the art. In response, Patent Owner asserts that *Johnson* in view of *RFC 1034* does not "disclose or suggest that the name of the secure mail server 16 can be a secure domain name." Response at 71. Patent Owner is incorrect. The Request explains that a person of ordinary skill in the art would have found motivation within *Johnson* to modify the secure communications disclosed therein to incorporate additional mechanisms to facilitate interbusiness communications by making it possible to locate the secure name server 14 by name, for example, through the public resources of the Internet. Request at 273-74, 82-84. That person would have found in both *Johnson* and *RFC 1034* an identification of the same problem (improving access of interbusiness communications) as well as a solution to the same problem: a user-friendly naming scheme. Consequently, the Examiner's rejection of claim 3 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

5. Dependent Claim 7

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* discloses every limitation of dependent claim 2. In response, Patent Owner asserts that *Johnson* does not disclose or suggest "that the registration process changes if the secure name server 14 and the secure mail server 16 reside on the same computer system." Response at 72. In particular, Patent Owner contends that, even when the secure name server and secure mail server reside on the same machine, they would "still communicate over the network *via the two separate* *communication lines*." Response at 72. Patent Owner's theories about how the secure name server and mail server in Johnson function might *communicate* over the Internet are both incorrect and irrelevant to the claims. Claim 7, in particular, does not impose any restrictions how the secure and non-secure communications may be "supported" by the specified device. As the Request explains, *Johnson* states that in certain circumstances, it would be appropriate to have the secure name server reside on the same machine as the secure mail server. Request at 287. *Johnson* explains in that scenario, certain lines of communications would remain encrypted, but does not show that the communications between the secure name server and secure mail server during registration must be secure. *Johnson* at col.11, ll.21-37; *see also* col.7, l.49 – col.8, l.24. Moreover, *Johnson* expressly indicates that the object of its systems is "to provide for a system which can communication [sic] on both secure and non-secure electronic mail servers." Accordingly, the Examiner's rejection of this claim was proper and should be maintained.

6. Dependent Claims 9-11 and 13-16

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered obvious dependent claims 9-11 and 13-16. In response, Patent Owner asserts that a person of ordinary skill would not be motivated to combine *Johnson* with *RFC 2401* because "it would change the principle of operation of *Johnson's* system." Response at 72. Patent Owner is incorrect. As explained in the Request, a person of ordinary skill in the art would have found motivation within *Johnson* to modify the secure communications disclosed therein to incorporate additional security mechanisms for communications over the Internet. Request at 289-90. That person would find in *Johnson* or *RFC 2401* identification of the same problem (improving security for Internet Protocol communications) as well as a solution to the same problem: an encryption and/or tunneling scheme. There is nothing in either reference that suggests that one must modify the essential features of the Johnson system to implement IPSec in communications.

Because Patent Owner provides no substantive response to claims 9-11 and 13-16, the Examiner's rejection of those claims based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

7. Dependent Claim 21

The Examiner properly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered claim 21 obvious. In response, Patent Owner presents no response distinct from its response relative to claim 1. Because the rejection of that claim was proper, the

Examiner's rejection of claim 21 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained. *See also* Request at 297-299.

8. Dependent Claim 22

The Examiner properly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered claim 21 obvious. In response, Patent Owner contends that the Request fails to "address the claimed feature of the secure name being registered 'prior to the step of sending a message to a secure name service.'" Response at 73. Patent Owner simply ignores the Request, which clearly explains that the secure email server will "go on to register the dynamic address" of the secure email server 16. *See also* Request at 299-300. This step, of course, would necessarily take place prior to another device securely communicating with secure email server 16. Consequently, the Examiner's rejection of claim 21 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

9. Independent Claim 24

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render claim 24 invalid. In response, the only new argument presented by Patent Owner is that the Request "has things reversed, as the claim recites 'sending a message securely from the first device to the second device." Response at 74. Patent Owner is incorrect. As already demonstrated above, certainly Patent Owner would agree that *Johnson* does not disclose a system that only permits one-way communication—and neither does the '181 patent, for that matter—such that the so-called "first device" of *Johnson* may be deemed a "second device" within the context of the claim depending upon which device initiates the secure communication. Accordingly, the Examiner's rejection of the claim was proper and should be maintained. *See also* Request at 301-304.

10. Dependent Claim 25

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render claim 25 invalid. In response, Patent Owner asserts only that "[t]he Office and Requester completely fail to address" the claim requirement of "sending a message securely . . . using a secure communication link." Response at 74. Patent Owner is incorrect. As explained in the Request, "the dynamic address of the secure electronic mail server 16 is not easily obtained" because, for example, it requires "<u>authorization to access and is protected through encryption</u>." Request at 304-05. Thus, *Johnson* describes "sending a message securely …

using a secure communication link." Accordingly, the Examiner's rejection of the claim was proper and should be maintained.

11. Independent Claim 26 and Dependent Claim 27

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render claims 26 and 27 invalid. Patent Owner presents no response distinct from its response to the rejection of claim 1. Accordingly, because the rejection of that claim was proper, the Examiner's rejection of claims 26 and 27 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained. *See also* Request at 305-314.

12. Independent Claim 28

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render claim 28 invalid. Patent Owner presents no response to claim 28 distinct from its response to the rejection of claims 1 and 2. Accordingly, because the rejections of claims 1 and 2 were proper, the Examiner's rejection of claim 28 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained. *See also* Request at 314-317.

13. Independent Claim 29

The Examiner correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render claim 29 invalid. Patent Owner presents no response to claim 29 distinct from its response to the rejection of claims 1 and 2. Accordingly, because the rejections of those claims were proper, the Examiner's rejection of claim 29 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained. *See also* Request at 317-318.

K. There are No Secondary Considerations Linked to the Claims

Patent Owner provides alleged evidence of secondary considerations to respond to obviousness rejections imposed on the claims. The putative evidence is nothing more than unsupported statements by its own Chief Technology Officer, Robert Short that should be disregarded as being obviously biased. Moreover, these self-serving statements should be disregarded because they do not correlate any evidence of commercial success of the specifically attributable to the claimed invention – a bedrock precondition of finding evidence of secondary indicia of non-obviousness relevant to the question of obviousness (i.e., of the <u>claimed</u> invention).

The specific assertions made by Patent Owner and its employee are also substantively irrelevant to the claims. First, Patent Owner contends that there was "long-felt need for easily enabled secure communications" because "remove access was 'a nightmare' for support desks, and adding the commercially available VPN software was even more difficult." Response at 76. However, Patent Owner has not demonstrated that claimed invention, rather than the prior art DNS systems taught in the prior art (e.g., *Beser, Mattaway, H.323, Johnson, Provino or Lendenmann* or combinations thereof) are responsible for addressing these long-felt needs.

Similarly, the Patent Owner contends there is evidence of significant commercial success. Initially, the putative evidence of commercial success is not evidence of commercial success of any product or service. Instead, Patent Owner refers only to licensing revenue – which is not probative of commercial success of any claimed method or system. In addition, Patent Owner provides no evidence that establishes that whatever commercial success the Patent Owner's company has experienced—which is apparently limited solely to licensing revenue—is attributable to the features of the claimed invention. Plainly it is not. Consequently, the self-serving, non-objective statements of its employee simply are not evidence of secondary indicia of non-obviousness, much less is probative evidence of the commercial success of the methods or systems that are claimed. Consequently, the Office should disregard these statements and give them no weight in assessing the obviousness of the claimed methods and articles.

L. Conclusions

As is evident from its responses to each of the rejections imposed by the Office, Patent Owner's arguments are uniformly based on its belief that the patent claims expressly incorporate a large number of limitations and requirements. The basis for that belief is plainly not the claim language. For example, Patent Owner frequently points to its theory of how its invention functions, what it believes is described in the '181 patent, or, simply, what it wishes its invention to be. Similarly, in criticizing the teachings in the prior art, Patent Owner frequently resorts to putative distinctions between the systems and methods of the claims and those being described in the prior art. Again, however, those criticisms rest on hypothetical claims that do not correspond to the actual claims of the '181 patent. Requester, thus, urges the Office to maintain the rejections, as they are based on the broadest reasonable construction of the actual claim language used in the claims of the '181 patent, and not the Patent Owner's hypothetical claims or concepts.

Consequently, based on the reasons set forth above, the Requester submits that the Patent Owner has not rebutted the Examiner's rejections of the claims on any of Issues 1-13 of Office Action of June 4, 2012. The rejection of all the claims under each of those Issues should, accordingly, be maintained.

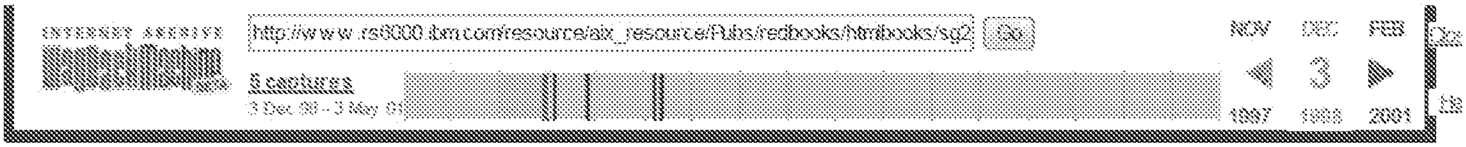
Respectfully submitted,

/ Jeffrey P. Kushan /
Reg. No. 43,401
Attorney for Third Party Requester

SIDLEY AUSTIN LLP
1501 K Street, N.W
Washington, D.C. 20005

tel. (202) 736-8000/ fax (202) 736-8711
Date: October 22, 2012

EXHIBIT A



http://www.rs6000.ibm.com/resource/aix_resource/Pubs/redbooks/htmlbooks/sg2

Contents

Directory Service

Security Service

Threads

EXHIBIT B

ational
nication

Highlights
Radiocommunication
Standardization
Development
TELECOM Events
Publications
Databases
Search

Table of Contents and Summary of Recommendation H.323 (02/98)

Download

Availability: Public

View or Download Document

	Format	Size	Posted	Download
English	HTML	30.0 kb	Aug 03 1998	⬇

Home | Search | Site Map | Help | Contact | Comments | © Copyright

English | Français | Español

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of	)	
U.S. Patent No. 8,051,181	)	Control No.: 95/001,949
Victor Larson et al.	)	Group Art Unit: 3992
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF SERVICE

I hereby certify that a copy of this correspondence for Comments by Third Party Requester Pursuant to Under 37 C.F.R. § 1.947 has been served in its entirety by First Class Mail on the following:

VirnetX Inc.
c/o McDermott Will & Emery
600 13th Street, N.W.
Washington, D.C. 20005-3096

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Reg. No. 43,401
October 22, 2012

Electronic Acknowledgement Receipt

EFS ID:	14047367
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	23630
Filer:	Karen L. Knezek./Jennifer Gordon
Filer Authorized By:	Karen L. Knezek.
Attorney Docket Number:	41484-80200
Receipt Date:	22-OCT-2012
Filing Date:	28-MAR-2012
Time Stamp:	18:57:09
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Third Party Requester Comments after Non-final Action	Comments_by_Third_Party_Requester_Pursuant_to_37_CFR_1947_flat.pdf	5243818 5e69fdc8052fb24d6fb24351bab30f7de13e0249	no	49

Warnings:

Information:

2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Exhibit_A_Understanding_OSF_DCE_flat.pdf	697772 bb6681c70ddb351f98ffea398b1331df9634bbda	no	7
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Exhibit_B_Table_of_Contents_and_Summary_of_Recommendation_H323_flat.pdf	117168 3804778cba907e82240776788978b82879efdf28	no	2
Warnings:					
Information:					
4	Reexam Certificate of Service	Certificate_of_Service_flat.pdf	81418 241f8ed30a37a7144fd26f8b5cdb5f0e2f558ce4	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	6140176		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor LARSON et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)))	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

REVOCATION OF POWER OF ATTORNEY, STATEMENT UNDER 37 C.F.R. § 3.73(b), AND GRANT OF NEW POWER OF ATTORNEY

The undersigned, a representative authorized to sign on behalf of the assignee owning all of the interest in U.S. Patent No. 8,051,181 ("the '181 patent"), hereby revokes all previous powers of attorney or authorization of agent granted in the '181 patent before the date of execution hereof.

In compliance with 37 C.F.R. § 3.73(b), the undersigned verifies that VirnetX Inc. is the assignee of the entire right, title, and interest in the '181 patent by virtue of an assignment recorded in the U.S. Patent and Trademark Office at Reel 019464, Frame 0133 on June 21, 2007.

The undersigned representative of the assignee hereby grants its power of attorney to the patent practitioners associated with **Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Customer Number 22,852**, to transact all business in the Patent and Trademark Office connected with the '181 patent, including the reexamination proceedings assigned control no. 95/001,949, and in any other proceedings involving the '181 patent.

Please also send all future correspondence concerning the '181 patent to the address associated with **Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Customer Number 22,852.**

Dated: 11/30/12

By: ______________________
Sameer Mathur
Vice President, Corporate Development and Product Marketing
VirnetX Inc.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor LARSON et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)))	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Revocation of Power of Attorney, Statement Under 37 C.F.R. §3.73(b), and Grant of New Power of Attorney was served by first-class mail on December 3, 2012, on counsel for the third party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 3, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14369775
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	23630
Filer:	Joseph Edwin Palys./connie sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	03-DEC-2012
Filing Date:	28-MAR-2012
Time Stamp:	16:43:33
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ReExam_POA_949.pdf	84731 7db112ea38703103db8175ab503883920c6fb2f1	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Reexam Change in Pwr Atty for Third Party Requester	1	2
	Reexam Certificate of Service	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	84731	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,949	03/28/2012	8051181	41484-80200

CONFIRMATION NO. 4522

POA ACCEPTANCE LETTER

OC000000057957994

22852
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

Date Mailed: 12/04/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/03/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/sdstevenson/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,949	03/28/2012	8051181	41484-80200

CONFIRMATION NO. 4522

POWER OF ATTORNEY NOTICE

OC000000057957945

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Date Mailed: 12/04/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/03/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/sdstevenson/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 4522

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
95/001,949	03/28/2012 RULE	709	3992	41484-80200

APPLICANTS

8051181, Residence Not Provided;
VIRNETX INC.(OWNER), ZEPHYR COVE, NV;
JEFFREY P. KUSHAN(3RD.PTY.REQ.), WASHINGTON, DC;
APPLE INC.,(REAL PTY IN INTEREST), CUPERTINO, CA;
SIDLEY AUSTIN LLP, DALLAS, TX

** **CONTINUING DATA** *************************

This application is a REX of 11/679,416 02/27/2007 PAT 8051181
which is a CON of 10/702,486 11/07/2003 PAT 7188180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6502135
which is a CIP of 09/429,643 10/29/1999 PAT 7010604
which claims benefit of 60/106,261 10/30/1998

** **FOREIGN APPLICATIONS** ********************

Foreign Priority claimed □ yes □ no
35 USC 119 (a-d) conditions met □ yes □ no □ Met after Allowance
Verified and Acknowledged ____________________
Examiner's Signature Initials

STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS

ADDRESS
22852

TITLE
METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

FILING FEE RECEIVED

FEES: Authority has been given in Paper
No. _________ to charge/credit DEPOSIT ACCOUNT
No. _________ for following:

□ All Fees
□ 1.16 Fees (Filing)
□ 1.17 Fees (Processing Ext. of time)
□ 1.18 Fees (Issue)
□ Other ______________
□ Credit

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No.	**8,051,181**	))	Control No.:	**95/001, 949**
Inventors:	Larson et al.	))	Examiner:	**Dennis Bonshock**
		))	Group Art Unit: 3992	
		))	Confirmation No. 4522	
		)		

Mail Stop *Inter Partes* Reexam
ATTN: Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

PETITION UNDER 37 CFR §1.182 TO ALIGN SCHEDULES OF RELATED PROCEEDINGS

Third Party Requestor Apple Inc. ("Petitioner") petitions under 37 CFR § 1.183 to request that the Office take actions to accelerate, and to thereby better align, the schedules of Reexamination Control No. 95/001, 949 with the schedules of 95/001,788 and 95/001,789.[1] Doing so will serve the interests of justice by facilitating the concurrent review by the Federal Circuit of related issues of patentability if final decisions in the three proceedings are appealed. Doing so will also help ensure that the outcomes of the Office proceedings will be considered in conjunction with outcomes in concurrent litigation concerning the same patents. Finally, accelerating the proceedings will effectuate the statutory mandate of conducting *inter partes* reexamination proceedings with special dispatch.

[1] Petitioner earlier filed a form of this document that included references on the title page to two other related proceedings in which ACP's had not yet issued. Petitioner was advised by the Office to remove the references to other control numbers in this petition, and resubmit each petition individually. Through this filing, Petitioner is withdrawing the previously submitted petition that referenced multiple control numbers.

I. Background

1. Reexamination Control No. 95/001,682 was ordered on October 3, 2011, and concerns U.S. Patent No. 6,520,135. The Office issued an Office Action in the '682 proceeding[2] rejecting claims 1-18 of the '135 patent on February 15, 2012. Patent Owner responded to the '682 Office Action on May 15, 2012, and Requester timely filed a reply on October 4, 2012.

2. Reexamination Control No. 95/001,697 was ordered on October 21, 2011, and concerns U.S. Patent No. 7,490,151. The '697 proceeding was merged with Reexamination Control No. 95/001,714 on March 15, 2012. The Office issued an Office Action in the '697 proceeding on April 20, 2012 rejecting claims 1-30 of the '151 patent. Patent Owner responded to the '697 Office Action on July 20, 2012, and Requester timely filed a reply on October 25, 2012.

3. Reexamination Control No. 95/001,788 was ordered December 29, 2011, and concerns U.S. Patent No. 7,418,504. The Office issued an Office Action in the '788 proceeding on December 29, 2011, rejecting claims 1-60. Patent Owner responded to the Office Action on March 29, 2012, and Requester timely filed a reply on June 25, 2012. The Office issued an Action Closing Prosecution (ACP) in the '788 proceeding on September 26, 2012. In response to a petition from Patent Owner, the deadline for responding to the ACP was extended to December 26, 2012.

4. Reexamination Control No. 95/001,789 was ordered December 29, 2011, and concerns U.S. Patent No. 7,921,211. The Office issued an Office Action in the '789 proceeding on January 18, 2012, rejecting claims 1-60. Patent Owner responded to the '789 Office Action on April 18, 2012, and Requester timely filed a reply on August 6, 2012. The Office issued an ACP in the '789 proceeding on September 26, 2012. In response to a petition from Patent Owner, the deadline for responding to the ACP was extended to December 26, 2012.

[2] In this petition, the last three digits of the control number of each proceeding are used to identify the proceeding.

5. Reexamination Control No. 95/001,949 was ordered June 4, 2012, and concerns U.S. Patent No. 8,051,181. The Office issued an Office Action in the '949 proceeding on June 4, 2012, rejecting claims 1-29. Patent Owner responded to the Office Action on September 4, 2012, and Requester timely filed a reply on October 22, 2012.

6. Each of the '135, '151, '504, '211 and '181 patents claims priority to, *inter alia*, U.S. Provisional Application No. 60/106,261.

7. There is a substantial overlap in the disclosures of the '135, '151, '504, '211 and '181 patents.

8. One or more claims in the '135, '151, '504, '211 and '181 patents has been rejected for anticipation or as being obvious over, *inter alia,* Aventail Connect v3.1, Aventail Connect v3.01, Aventail AutoSOCKS, Proxies for Anonymous Routing ("Reed"), Broadband Forum TR-025: Core Network Architecture Recommendations for Access to Legacy Data Networks Over ADSL ("Wang"), BinGO! User's Guide ("BinGO"), Flexible Internet Secure Transactions based on Collaborative Domains ("Solana"), Understanding OSF DCE 1.1 for AIX and OS/2 ("Lendenmann"), RFC 2230, RFC 2538, H.323, U.S. Patent No. 6,557,037 to Provino, U.S. Patent No. 6,496,867 to Beser, U.S. Patent No. 6,131,121 to Mattaway, and U.S. Patent No. 6,499,108 to Johnson.

9. The '135, '151, '504 and '211 patents are the subject of Civil Action No. 6:2010cv00417 initiated by the Patent Owner in the Eastern District of Texas (the "Texas litigation").

10. The '181 patent is the subject of ITC investigation 337-TA-858 currently set for hearing on July 10, 2013.

11. On November 6, 2012, a jury issued a verdict in the Texas litigation (Civil Action No. 6:2010cv00417) finding certain claims in the '135, '151, '504 and '211 patents infringed by Petitioner and not invalid. Specifically, the jury verdict addressed only claims 1, 3, 7, and 8 of the '135 patent, claims 1 and 13 of the

'151 patent, claims 1, 2, 5, 16, 21, and 27 of the '504 patent, and claims 36, 37, 47, and 51 of the '211 patent.

12. No final judgment has been entered by the Court in Civil Action No. 6:2010cv00417 as of the date of this Petition.

II. Relief Requested

This petition is presented under 37 CFR § 1.182, as it requests relief not provided for by any other rule.

Petitioner requests the Office to act promptly in issuing an Action Closing Prosecution in the '949 proceeding, and to limit the period granted in that proceeding for Patent Owner and/or Requestor to respond to the ACP to no more than one month, and to take such other steps that will expedite issuance of a final decision in each of the three pending reexamination proceedings. Doing so will help align the schedules of the '949 proceeding with those of the '788 and '789 proceedings, in which ACPs have issued with a previously extended deadline for response of December 26, 2012 for each proceeding.

III. Argument

Taking this action in the '949 proceeding serves the public interest, and is consistent with the Office's statutory mandate in 35 U.S.C. § 314 to conduct *inter partes* reexamination proceedings with "special dispatch."

The three patents that are the subject of the '949, '788 and '789 proceedings are closely related. Each claims priority to or benefit of one or more of the same, earlier filed applications, and the disclosures in the three patents are substantially similar. Moreover, claims in the three patents have been found to be anticipated by or would have been obvious in view of several of the same patents and printed publications. The three proceedings thus present similar and related issues of patentability over the prior art.

Taking steps to better align the schedules of the three proceedings will serve the public interest by providing for an efficient and expeditious review of final decisions of the Office concerning the three related patents. Most importantly, it will minimize the burden on the Federal Circuit in the event that appeals are taken by the Patent Owner or the Requestor from a final decision in the three different proceedings. As noted above, there is a substantial overlap in the disclosure in the patents, and similar patentability issues exist in each proceeding. Requiring the Federal Circuit to review these similar disclosures and patentability issues in distinct and time-separated appeals would be inefficient and burdensome on the Court.

Expediting the conclusion of the '949 proceeding will also enable appeals of the three patents to be considered concurrently with any appeal arising from concurrent litigation pending in the Eastern District of Texas or International Trade Commission. As noted above, on November 6, 2012, a jury in the Texas litigation issued a verdict finding the asserted claims of the '504 and '211 patents not invalid and infringed by Requestor. Judgment has not been entered in the Texas litigation as of the present date. Though the '181 patent was not implicated in that litigation, an appeal arising out of the Texas litigation thus will likely overlap with one or more of the current reexamination proceedings both in time and in the issues raised. Further, the '181 patent is the subject of an International Trade Commission investigation set for hearing on July 13, 2013. Again, the Office should take actions in its power to avoid burdening the Federal Circuit with multiple, time-separated appeals on related patents that present similar patentability issues.

In this latter respect, Petitioner observes that not all of the claims being addressed in the three *inter partes* reexamination proceedings were asserted by Patent Owner in the Texas litigation.[3] Thus, several claims in each patent will require review by the Federal Circuit regardless of the outcome of the Texas litigation or an appeal from it. Petitioner also notes that Patent Owner has recently commenced additional actions for infringement of the three patents at issue in the '949, '788 and '789 proceedings, including an action filed on November 6 of this year in the Eastern District of Texas (i.e., Civ. Act. 6:2012cv00855 (E.D. Tex.) and a complaint filed in the International Trade Commission on September 14, 2012 (337-TA-858). Petitioner also notes that the '504 and '211

[3] Patent Owner has asserted in the Texas litigation that a judgment should be rendered on the validity of all of the claims in each patent, even though it has not asserted infringement of each of those claims. Requestor has moved to dismiss its counterclaim of invalidity of non-asserted claims in each patent, as jurisdiction does not exist for these non-asserted claims. The Court has taken Requestor's motion under advisement, but has not issued a decision as of the date of this petition.

patents are scheduled to be tried to a jury in March 2013. The Court and the jury will consider the invalidity of several claims in each of the patents in that trial, as will the ITC.

The interests of judicial efficiency are served by enabling the concurrent review of decisions of the Office and of the Federal Courts of the same patents, and on similar issues of patentability. The Office also acts under an independent statutory mandate to review patentability issues, and does so independently of the district courts. See *In Re Translogic Technology,* 504 F.3d 1249 (Fed. Cir. 2007) (considering appeal from reexamination proceeding despite appeal from district court on same patent). The interests of judicial efficiency and the public interest in expeditious completion of *inter partes* reexamination proceedings are best served by accelerating the '949 proceeding.

Accelerating the '949 proceeding is also the only path consistent with the Office's mandate to conduct *inter partes* reexamination proceedings with special dispatch. In this respect, delaying the '788 and '789 proceedings to better align the three proceedings would be contrary to the Office's mandate to handle the proceedings with special dispatch. For example, there is no Court order or other mandate relevant to the Office concerning these patents. Moreover, the '949 proceeding has been fully briefed since October, and is ripe for final action by the Office.

Accelerating the '949 proceeding also will not prejudice the interests of the Patent Owner. Patent Owner has sought and been granted extensions of time to respond to the issues raised in each proceeding. Patent Owner also is fully aware of the patentability issues raised in the '181 patent that is the subject of the '949 proceeding. And, of course, there is a substantial overlap in the prior art and patentability issues raised in each proceeding.

IV. Conclusion

For the foregoing reasons, Petitioner requests the Office to: (i) promptly issue actions closing prosecution in the '949 proceeding, (ii) set a one month or shorter period for Patent Owner and/or Requester to respond to the ACP, and (iii) take such other actions that are appropriate to expeditiously conclude the '949, '788 and '789 proceedings.

The Director is authorized to charge the fee specified in 37 CFR § 1.20(c)(6) to Deposit Account No. 18-1260. In addition, the Director is authorized to charge any other fee he deems necessary to Deposit Account No. 18-1260.

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requestor

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile

December 5, 2012

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 8,051,181		)	Control No.: 95/001,949
Filed:	February 27, 2007	)	Group Art Unit: 3992
Issued:	November 1, 2011	)	Examiner: Dennis Bonshock
Inventors:	Larson et al.	)	Confirmation No. 4522
For:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

REQUEST FOR REFUND

Petitioner Third Party Requestor Apple, Inc. hereby requests a refund of $400.00 for the fee paid under 37 C.F.R. § 1.17(f) for the "Petition under 37 C.F.R. §1.182 to Align Schedules of Related Proceedings" filed on November 29, 2012.

Filed concurrently herewith is a resubmitted "Petition under 37 C.F.R. §1.182 to Align Schedules of Related Proceedings" which withdraws the earlier filed petition and authorizes payment of the petition fee under 37 C.F.R. § 1.20(c)(6) in the amount of $1,930.

It is requested that the Office credit Deposit Account No. 18-1260 in the amount of $400. If, in the resolution of this matter, further documents and/or evidence are required, it is requested that the Office either call or write the undersigned.

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requestor

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005

(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile
December 5, 2012

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 8,051,181	)	Control No.: 95/001,949
	)	
Filed: February 27, 2007	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis Bonshock
	)	
Inventors: Larson et al.	)	Confirmation No. 4522
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	))))	

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF SERVICE

I hereby certify that a copy of this correspondence for Petition under 37 C.F.R. §1.182 to Align Schedules of Related Proceedings and Request for Refund has been served in its entirety by First Class Mail on the following:

McDERMOTT WILL & EMERY
600 13th Street, NW
Washington, DC 20005-3096

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requestor

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile
December 5, 2012

DA1 680033v.1

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Karen L. Knezek.
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION IN REEXAM PROCEEDING	1824	1	1930	1930
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**1930**

Electronic Acknowledgement Receipt

EFS ID:	14388961
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Karen L. Knezek.
Filer Authorized By:	
Attorney Docket Number:	41484-80200
Receipt Date:	05-DEC-2012
Filing Date:	28-MAR-2012
Time Stamp:	14:05:55
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1930
RAM confirmation Number	453
Deposit Account	181260
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Receipt of Petition in a Reexam	95001949_Petition_to_Synchronize_Virnetx_IPRs.pdf	140075 1fed621a08c828968a2e0c7a46b78d96d8175b81	no	7
Warnings:					
Information:					
2	Refund Request	95001949_request_refund.pdf	75574 afe154481d2a8f7e4abb3e6b458d283f670b374a	no	2
Warnings:					
Information:					
3	Reexam Certificate of Service	95001949_certificate_of_service.pdf	73563 f3b4af4b6341abe0b78499c5d97be2fd97d310e4	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	29995 ba558b3b0c3e6cc12e834dca1394e95f8500ecdb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	319207		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket Nos. 11798.0009, 0002, 0010, 0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

)
In re U.S. Patent No. 6,502,135) Control No.: 95/001,682
Edmund Munger et al.) Examiner: Behzad Peikari
)
)
In re U.S. Patent No. 7,490,151) Control Nos.: 95/001,697
Edmund Munger et al.) 95/001,714
) Examiner: Michael Yigdall
)
In re U.S. Patent No. 8,051,181) Control No.: 95/001,949
Victor Larson et al.) Examiner: Dennis Bonshock
)

VIA EFS WEB

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S PETITION IN OPPOSITION TO THIRD-PARTY REQUESTER APPLE INC.'S PETITION TO ALIGN SCHEDULES

VirnetX Inc., the owner of the above-referenced patents, opposes third-party requester Apple Inc.'s Petition Under 37 CFR § 1.182 to Align Schedules ("Petition"). Apple's own delays are primarily responsible for the current progress of the reexaminations. Apple has also made several strategic decisions during these reexaminations that have slowed their schedules, and therefore Apple should not now be heard to complain that the reexaminations are not as advanced as Apple would now prefer. As a result, the relief sought in the Petition should not be granted, especially since it prejudices the patent owner VirnetX.

If entry and consideration of this petition requires suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. And if any fee is due in connection with the filing of this petition, please charge it to Deposit Account 06-0916.

I. Background

A. Control No. 95/001,682 ("the '1,682 proceeding")

Apple filed its Request for Reexamination of U.S. Patent No. 6,502,135 ("the '135 patent") on July 8, 2011. The Office granted the Request and ordered reexamination on October 3, 2011. The Office issued an Office Action on February 15, 2012. Patent Owner timely filed a Response to the Office Action on May 15, 2012, and Apple filed Comments on October 4, 2012.

B. Control Nos. 95/001,697 ("the '1,697 proceeding") and 95/001,714 ("the '1,714 proceeding")

Apple filed its Request for Reexamination of U.S. Patent No. 7,490,151 ("the '151 patent") on July 25, 2011. The Office granted the Request and ordered reexamination on October 21, 2011. The Office merged this proceeding on March 15, 2012 with a separate reexamination involving the '151 patent. That other reexamination bears control no. 95/001,714 and names Cisco Systems, Inc. ("Cisco") as the real party in interest. The Office issued an Office Action in the merged proceedings on April 20, 2012. Patent Owner timely filed a Response to the Office Action on July 20, 2012, and Apple filed Comments on October 25, 2012.

C. Control No. 95/001,788 ("the '1,788 proceeding")

Apple filed its Request for Reexamination of U.S. Patent No. 7,418,504 ("the '504 patent") on October 18, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on December 29, 2012. Patent Owner timely filed a response to the Office Action on March 29, 2012, and Apple filed Comments on June 25, 2012. The Office issued a second Office Action on September 26, 2012, which remains pending.

D. Control No. 95/001,789 ("the '1,789 proceeding")

Apple filed its Request for Reexamination of U.S. Patent No. 7,921, 211 ("the '211 patent") on October 18, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on January 18, 2012. Patent Owner timely filed a response to the Office Action on April 18, 2012, and Apple filed Comments on August 6, 2012. The Office issued a second Office Action on September 26, 2012, which remains pending.

E. Control No. 95/001,949 ("the '1,949 proceeding")

Apple filed its Request for Reexamination of U.S. Patent No. 8,051,181 ("the '181 patent") on March 28, 2012. The Office granted the Request, ordered reexamination, and issued an Office Action on June 4, 2012. Patent Owner timely filed a response on September 4, 2012, and Apple filed Comments on October 22, 2012.

F. Recent Jury Verdict in the Eastern District of Texas

Patent Owner asserted the '135, '151, and '504 patents in a Complaint filed against Apple on August 11, 2010 in the Eastern District of Texas (*VirnetX Inc. v. Cisco Sys., Inc., et al.*, No. 6:10-cv-00417). Patent Owner additionally asserted the '211 patent on the day it issued in an Amended Complaint filed against Apple on April 5, 2011.

The jury found the asserted claims of the '135, '151, '504, and '211 patents valid and infringed, awarding Patent Owner over $368 million in damages on November 6, 2012. (Ex. A-10.)

II. Argument

Faced with a recent adverse jury verdict, Apple brings its Petition to assert that the '1,682, '1,697, and '1,949 proceedings must be accelerated. (Petition 5-6.) However, the primary reasons the reexaminations lag so far behind the district-court action are Apple's own delays in filing its reexamination requests and its delays in responding to Patent Owner's filings. The Office should not grant the extraordinary relief sought by Apple for at least this reason and for the other reasons discussed below.

First, Apple did not begin to file these reexamination requests until eleven months after the litigation began, and delayed still longer in filing its other reexamination requests concerning additional VirnetX patents. Apple has been on notice of Patent Owner's infringement claims based on the '135, '151, and '504 patents at least since Patent Owner filed its first Complaint on

August 11, 2010. Yet Apple did not file requests for inter partes reexamination of the '135, '151, and '504 patents until July 8, 2011, July 25, 2011, and October 18, 2011, respectively. Due to Apple's delays of up to fourteen months in filing, the prosecution of these reexaminations is still before the Central Reexamination Unit. Apple has no basis to now request additional burdensome action on the part of the Office and the Patent Owner, having caused the very delays it seeks to remedy.

Second, these reexaminations are already being appropriately conducted by the Office with the "special dispatch" sought by Apple. In the '1,682, '1,697, and '1,949 proceedings, Apple filed enormous requests for reexamination totaling 423, 380, and 368 pages, respectively, including appended claim charts. These requests presented proposed rejections implicating over 30 different references—several of them well over one hundred pages long. (*See id.* at 3, listing 15 of these references.) The Office had to review and process all of these papers before issuing Office Actions, and did so within an expeditious timeframe. Apple could have honed its invalidity positions and filed more targeted reexamination requests to streamline these proceedings, but it did not. Apple elected to proceed with an omnibus approach to these reexaminations, and should not now be heard to complain about the Office's and Patent Owner's efforts in reviewing Apple's vast filings and advancing these reexaminations.

Third, Apple's own conduct during the '1,682, '1,697, and '1,949 proceedings has slowed their progress. For example, in the '1,682 proceeding, Apple did not file its Comments until October 4, 2012—almost five months after Patent Owner's response to the Office Action. In the '1,697 merged proceeding, Apple did not file its Comments until October 25, 2012, almost three months after Patent Owner's response to the Office Action. Similarly, in the '1,949 proceeding, Apple did not file its Comments until October 22, 2012, over a month and a half after Patent Owner's response to the Office Action. In each of these instances, Apple has delayed almost as long as possible before filing its Comments. For example, in the '1,682 proceeding, Apple filed a petition to strike Patent Owner's response for exceeding the 50-page limit in responding to Apple's request and claim charts totaling 423 pages, which then delayed Apple's filing of its Comments until the petition was denied, slowing the schedule by five months. These are not the actions of a party preeminently concerned with the speed of these proceedings.

Fourth, Apple's impatience with the current progress of the '1,682, '1,697, and '1,949 proceedings is misplaced. Due in part to Apple's various delays in filing its Comments, the Office has only had both parties' briefing on the first Office Action in the '1,682 proceeding for two months, and a little over one month for the first Office Actions in the '1,697, and '1,949 proceedings. By comparison, Apple took five, two, and one and a half months, respectively, to respond to Patent Owner's Office Action responses alone. In total, the parties' combined briefing ranges from 123 to 192 pages in each proceeding, and the briefing further discusses and responds to the enormous number of issues raised in Apple's lengthy reexamination requests. Asking the Office to "promptly" produce second Office Actions in these proceedings is therefore inappropriate. (*Id.* at 7.)

Fifth, contrary to Apple's representations, accelerating the '1,682, '1,697, and '1,949 proceedings would substantially prejudice Patent Owner. In addition to these reexaminations, Apple is also named as the real party in interest in two other similarly expansive reexaminations in the '1,788 and '1,789 proceedings, discussed above, which are currently demanding significant attention from Patent Owner. Patent Owner is also concurrently involved in six other reexaminations which name Apple's co-defendant Cisco, and these reexaminations are at a similar stage as the Apple-initiated reexaminations. (*See* control nos. 95/001,679; 95/001,746; 95/001,792; 95/001,851; 95/001,856 and the merged proceedings in control nos. 95/001,714 and 95/001,697.) Accelerating the '1,682, '1,697, and '1,949 proceedings would burden Patent Owner and its counsel given that it must also respond to filings from Apple and Cisco in a large number of other reexaminations. In addition, shortening the time period for response as Apple requests would further burden the Patent Owner and would not provide the Patent Owner adequate time and opportunity to respond.

Finally, accelerating these proceedings would not achieve efficiency before the Federal Circuit as advocated by Apple. Based on the jury's verdict on November 6, 2012, Patent Owner expects that the district court will enter a final judgment in the very near future, and as a result, the litigation will reach the Federal Circuit long before the reexaminations will. So, even if the Office were to grant Apple's request (which it should not), the reexaminations will not be ready for appeal to the Federal Circuit for quite some time.

III. Conclusion

The reexaminations are proceeding with the appropriate "special dispatch." Apple's complaints arise chiefly from its own delay in waiting to file its requests for reexamination until July and October 2011, as well as from its own strategic decisions during the course of these reexaminations. Moreover, granting Apple's request will only prejudice the Patent Owner. In view of all of the foregoing circumstances, Patent Owner respectfully submits that Apple's petition should be denied.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 13, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

EXHIBIT A-10

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX INC.,	§	
Plaintiff,	§	
vs.	§	**CASE NO. 6:10-CV-417**
APPLE INC.,	§	
Defendant.	§	

VERDICT FORM

In answering these questions, you are to follow all of the instructions I have given in the Court's Charge.

1. Did VirnetX prove by a preponderance of the evidence that Apple infringes the following claims of the following patents?

Answer "Yes" or "No" for each Claim.

'135 Patent

Claim 1 yes
Claim 3 yes
Claim 7 yes
Claim 8 yES

'151 Patent

Claim 1 yes
Claim 13 yes

'504 Patent

Claim 1 yes
Claim 2 yes
Claim 5 yes
Claim 16 yes
Claim 21 yes
Claim 27 yes

'211 Patent

Claim 36 yes
Claim 37 yes
Claim 47 yes
Claim 51 yes.

EXHIBIT A-10

2. Did Apple prove by clear and convincing evidence that the following listed claims of the following patents are invalid?

If you find the claim invalid, answer "Yes;" otherwise, answer "No."

'135 Patent

Claim 1	NO
Claim 3	NO
Claim 7	NO
Claim 8	NO

'151 Patent

Claim 1	NO
Claim 13	NO

'504 Patent

Claim 1	NO
Claim 2	NO
Claim 5	NO
Claim 16	NO
Claim 21	NO
Claim 27	NO

'211 Patent

Claim 36	NO
Claim 37	NO
Claim 47	NO
Claim 51	NO

3. What sum of money, if paid now in cash, do you find from a preponderance of the evidence would fairly and reasonably compensate VirnetX for Apple's infringement, if any, of the patents up to the time of trial?

Answer with the amount: $ 368,160,000.00

PATENT
Customer No. 22,852
Attorney Docket Nos. 11798.0009, 0002, 0010, 0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

)
In re U.S. Patent No. 6,502,135) Control No.: 95/001,682
Edmund Munger et al.) Examiner: Behzad Peikari
)
)
In re U.S. Patent No. 7,490,151) Control Nos.: 95/001,697
Edmund Munger et al.) 95/001,714
) Examiner: Michael Yigdall
)
In re U.S. Patent No. 8,051,181) Control No.: 95/001,949
Victor Larson et al.) Examiner: Dennis Bonshock
)

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Petition in Opposition to Third-Party Requester Apple's Petition to Align Schedules was served by first-class mail on December 13, 2012, on counsel for the third party requesters at the following addresses:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 13, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14462669
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	13-DEC-2012
Filing Date:	28-MAR-2012
Time Stamp:	17:13:00
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		OpptoApplesPetitiontoAlign.pdf	411484 be81e6973d3ac4b55ba1a9f3a2339bfb61d8402d	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Reexam - Opposition filed in response to petition	1	6
	Reexam Miscellaneous Incoming Letter	7	9
	Reexam Certificate of Service	10	10

Warnings:

Information:

Total Files Size (in bytes):	411484

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 01/16/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	PAPER NUMBER
3992	
MAIL DATE	DELIVERY MODE
01/16/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Transmittal of Communication to Third Party Requester *Inter Partes* Reexamination	Control No.	Patent Under Reexamination 8051181	
	Examiner DENNIS BONSHOCK	Art Unit 3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400 DALLAS, TX 75201

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination prceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

U.S. Patent and Trademark Office
PTOL-2070 (Rev. 07-04)

Paper No. 20121213

ACTION CLOSING PROSECUTION (37 CFR 1.949)	**Control No.** 95/001,949	**Patent Under Reexamination** 8051181
	Examiner DENNIS BONSHOCK	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on 04 September, 2012
Third Party(ies) on 22 October, 2012

Patent owner may once file a submission under 37 CFR 1.951(a) within 1 month(s) from the mailing date of this Office action. Where a submission is filed, third party requester may file responsive comments under 37 CFR 1.951(b) within 30-days (not extendable- 35 U.S.C. § 314(b)(2)) from the date of service of the initial submission on the requester. **Appeal cannot be taken from this action.** Appeal can only be taken from a Right of Appeal Notice under 37 CFR 1.953.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. □ Notice of References Cited by Examiner, PTO-892
2. ☒ Information Disclosure Citation, PTO/SB/08
3. □ _____

PART II. SUMMARY OF ACTION:

1a. ☒ Claims 1-29 are subject to reexamination.
1b. □ Claims _____ are not subject to reexamination.
2. □ Claims _____ have been canceled.
3. □ Claims _____ are confirmed. [Unamended patent claims]
4. □ Claims _____ are patentable. [Amended or new claims]
5. ☒ Claims 1-29 are rejected.
6. □ Claims _____ are objected to.
7. □ The drawings filed on _____ □ are acceptable □ are not acceptable.
8 □ The drawing correction request filed on _____ is: □ approved. □ disapproved.
9 □ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
□ been received. □ not been received. □ been filed in Application/Control No _____
10. □ Other _____

ACTION CLOSING PROSECUTION

This action addresses claims 1-29 of United States Patent Number: 8,051,181 (Larson et al.) for which it has been determined in the Order Granting Inter partes Reexamination mailed 6-4-2012 (hereinafter "Order") that a substantial new question of patentability was raised in the Request for *inter partes* reexamination filed on 3-28-2012 (hereinafter "Request").

This is an Action Closing Prosecution in response to the Patent Owner's response filed 9-4-2012 and the Third Party Requester's response filed 10-22-2012.

IDS

Where the IDS citations are submitted but not described, the examiner is only responsible for cursorily reviewing the references. The initials of the examiner on the PTO-1449 indicate only that degree of review unless the reference is either applied against the claims, or discussed by the examiner as pertinent art of interest, in a subsequent office action. See Guidelines for Reexamination of Cases in View of In re Portola Packaging, Inc., 110 F.3d 786, 42 USPQ2d 1295 (Fed. Cir. 1997), 64 FR at 15347, 1223 Off. Gaz. Pat. Office at 125 (response to comment 6).

Consideration by the examiner of the information submitted in an IDS means that the examiner will consider the documents in the same manner as other documents in Office search files are considered by the examiner while conducting a search of the prior art in a proper field of search. The initials of the examiner placed adjacent to the citations on the PTO-1449 or PTO/SB/08A and 08B or its equivalent mean that the information has been considered by the examiner to the extent noted above.

Regarding IDS submissions MPEP 2656 recites the following: "Where patents, publications, and other such items of information are submitted by a party (patent owner or requester) in compliance with the requirements of the rules, the requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information."

Accordingly, the IDS submission on 9-20-2012 has been considered by the Examiner only with the scope required by MPEP 2656, unless otherwise noted.

Rejections Proposed by the Requester

A total of 12 references have been asserted in the Request as providing teachings relevant to the claims of the Larson patent. In view of the Order, 10 of the proposed issues have established a reasonable likelihood that the Requester will prevail. The following proposed rejections are the main issues to be discussed below:

Issue 1: Claims 1-12 in view of Beser

Issue 3: Claims 1, 2, 6-9, 12, 14-17, 19-21, and 24-29 in view of Mattaway

Issue 4: Claims 3-4, 10-11, 18, and 23 in view of Mattaway in view of Beser

Issue 5: Claims 10 and 11 in view of Mattaway in view of RFC2401

Issue 6: Claims 1-9, 12-15, and 18-29 in view of Lendenmann

Issue 7: Claims 10, 11, and 17 in view of Lendenmann in view of Beser

Issue 8: Claims 10 and 11 in view of Lendenmann in view of RFC2401

Issue 9: Claims 1-15, 18-23, 28, and 29 in view of Provino

Issue 10: Claims 24-26 in view of Provino in view of H.323

Issue 11: Claims 1-29 in view of H.323

Issue 13: Claims 1-16 and 18-29 in view of Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401

Claim Rejection Paragraphs

Claim Rejections - 35 USC § 102

The following are quotations from the MPEP regarding the types of rejections to be utilized below:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Issue 1

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-12, 14, 15, and 17-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-12, 14, 15, and 17-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Beser (see pages 23-40, 41-42, and 43-65 of the Request and pages 1-8 of the Exhibit C1 '181 Patent Claim Charts, incorporated by reference).

Issue 3

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1, 2, 7-9, 12-17, 19-21, and 24-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1, 2, 7-9, 12, 14-17, 19-21, and 24-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Mattaway (see pages 68-94 of the Request and pages 1-8 of Exhibit C2 '181 Patent Claim Charts, incorporated by reference).

Claim 13 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 76 of the Request and pages 4 of Exhibit C2 '181 Patent Claim Charts, incorporated by reference), the Requester lacked a citation to go alone with the quote they cited from the Mattaway reference, which is being herein supplemented by the Examiner.

> *Mattaway discloses that each call, i.e., session, "may be assigned a successive session number in sequence, which may be used by the respective processing unit to associate the call with one of the SLIP/PPP lines, to associate a <ConnectOK> response signal from a <ConnectRequest> signal, and to allow for multiplexing and demultiplexing of inbound and outbound conversations on conference lines .... " (see column 6, lines 24-36)*

Issue 4

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 3-4, 10-11, 18, and 23 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 3-4, 10-11, 18, and 23 are rejected under 35 U.S.C. 103(e) as being obvious over Mattaway in view of Beser (see pages 94-98 of the Request, incorporated by reference).

Issue 5

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10 and 11 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10 and 11 rejected under 35 U.S.C. 103(e) as being obvious over Mattaway in view of RFC2401 (see pages 98-100 in the Request, incorporated by reference).

Issue 6

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-9, 12-15, and 18-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-9, 12-15, and 18-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Lendenmann (see pages 101-159 of the Request and pages 1-7 of Exhibit C3 '181 Patent Claim Charts, incorporated by reference).

Issue 7

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10, 11, and 17 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10, 11, and 17 are rejected under 35 U.S.C. 103(e) as being obvious over Lendenmann in view of Beser (see pages 160-164 of Request, incorporated by reference).

Issue 8

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10 and 11 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10 and 11 are rejected under 35 U.S.C. 103(e) as being obvious over Lendenmann in view of RFC 2401 (see pages 164-166 of the Request, incorporated by reference).

Issue 9

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-15, 18-23, 28, and 29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-12, 18-23, 28, and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Provino (see pages 167-203 of the Request and pages 1-8 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference).

Claim 13 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 3 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 1, lines 1-24:

> *The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection there between, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address*

> *resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The* ***external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device .***

This paragraph provides support for a plurality of communications being provided during the period when the secure connection channel is enabled.

Claim 14 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 4 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 5, lines 28-35:

> *If the received message packets contain information, such as* ***Web pages or the like****, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit.* ***In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.***

This paragraph provides support for a plurality of different services being provided.

Claim 15 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 4 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 1, lines 1-24:

> *The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection there between, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The* ***external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device .***

Provino teaches in column 5, lines 28-35:

> *If the received message packets contain information, such as* ***Web pages or the like****, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit.* ***In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.***

These paragraphs provide support for multiple sessions and a plurality of application programs.

Issue 10

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 24-26 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 24-26 are rejected under 35 U.S.C. 103(e) as being obvious over Provino in view of H.323 (see pages 188-203 of the Request, incorporated by reference).

Issue 11

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-9 and 12-29 are rejected under 35 U.S.C. 102(b) as being obvious over H.323 (see pages 204-268 of the Request and on pages 1-8 of Exhibit C5 '181 Patent Claim Charts, incorporated by reference).

Claims 10 and 11 are adopted with clarification, as additionally rejected under 35 U.S.C. 102(b) (see pages 230-231 of the Request and on page 3 of Exhibit C5 '181 Patent Claim Charts, incorporated by reference)., the Requester lacked an appropriate supporting citation to go alone with the anticipation claim made with respect to the H.323 reference, which is being herein supplemented by the Examiner.

H.323 teaches on page 59:

> ***In order to conserve resources, synchronize call signaling and control, and reduce call setup time, it may be desirable to convey H.245 messages within the Q.931 call signaling channel instead of establishing a separate H.245 channel. This process,***

***known as "encapsulation" or "tunneling" of H.245 messages**, is accomplished by utilizing the h245Control element of h323_uu_pdu on the call signaling channel, copying an encoded H.245 message as an octet string. When tunneling is active, one or more H.245 messages can be encapsulated in any Q.931 message. If tunneling is being utilized and there is no need for transmission of a Q.931 message at the time an H.245 message must be transmitted, then a FACILITY message shall be sent with h323-message-body set to empty.*

This paragraph provides support for tunneling.

Issue 13

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-16 and 18-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-16 and 18-29 are rejected under 35 U.S.C. 103(e) as being obvious over Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401 (see pages 270-318 of the Request and on pages 1-9 of Exhibit C6 ‘181 Patent Claim Charts in the Request, incorporated by reference).

RESPONSE TO ARGUMENTS

Patent Owner relies upon the Declaration of Angelos D. Keromytis, Ph.D. for support in much of the response. This document has been fully considered by the Office, although the Examiner largely does not agree with the Keromytis position.

A. Whether Certain References should be Considered Prior Art

Patent Owner argues "*The Office rejects claims 1-29 of the '181 patent as anticipated or obvious in view of several references. As explained below, however, the rejections are based on references that have not been properly established as being publically available before the effective filing date of the '181 patent and do not disclose or suggest the combination of features recited in the claims.*" As "*The Office and the Requester have not provided any evidence (such as by affidavit) that Lendenmann, RFC 2131, H.323, H.225.3, H.235, H.245, RFC 1334, or RFC 2431 (together the "Asserted Publications"), were publicly available or that they are printed publications."*

The Third party requester responds that:

Lendenmann:

> *"The Lendenmann reference, "Understanding OSF DCE 1.1 for AIX and OS/2," ("Lendenmann') was published by the IBM International Technical Support Organization in October 1995--well in advance of the earliest available priority date of the 'l 81 patent, and is therefore unquestionably prior art under 35 U.S.C. § 102(b). Indeed, as indicated on its face, the Lendenmann reference was published in October 1995 as part of IBM's well known "redbook" collection. It was cataloged as redbook number SG24-4616 and, as described on page xxi,*

was made publicly available on the Internet at: http://www.redbooks.ibm.com/redbooks. As further evidence of its publication, the Internet Archive ("the Wayback Machine") shows that the document was publically available on the IBM website no later than December 3, I998, as indicated on Exhibit A. "

H.323, H.225.0, H.235, H245

"*The ITU-T H.323 Core Recommendations are a series of protocols that are published by the ITU Telecommunication Standardization Sector (ITU-T)--an organization that dates back to 1865--whose mission is to ensure the efficient and timely availability of standards deemed essential to the telecommunications industry. The face of these documents shows they were approved and made available publically no later than February. of 1998, As further evidence, the Wayback Machine shows that the recommendations were posted to the ITU website no later than ~. Exhibit B. Thus, each of the H.323, H.225.0, [4..235, H.245 recommendations was publically disseminated and is prior art to the 181 patent."*

RFCs

RFC documents are published mad disseminated to the public by the Interact Engineering Task Force (IETF) pursuant to transparent and well-known procedures. Specifically: (i) each number assigned to an RFC is unique and is

> *not "re-used" if the subject matter in an RFC is revised or updated, (ii) the date each RFC is distributed to the public is listed the front page of the RFC, (iii) RFCs are distributed to the public over the Internet, via numerous protocols, (iv) each RFC is announced via are email distribution list on the date it is released to the public, and (v) FOZCs are maintained in numerous archives publicly accessible via the Internet. In fact,* ***Patent Owner itself cites several RFCs as "printed publications" in the '181 Patent****.*

The Examiner agrees with the third party requestor that these documents were printed publication available to the public prior to February 15, 2000. Internet documents are valid printed publications as MPEP 2128 states: *"An electronic publication, including an on-line database or Internet publication, is considered to be a "printed publication" within the meaning of 35 U.S.C.* ***102****(a) and (b) provided the publication was accessible to persons concerned with the art to which the document relates. See In re Wyer, 655 F.2d 221, 227, 210 USPQ 790, 795 (CCPA 1981)"*

B. Rejections Under Baser (ISSUE 1)

1. Overview

Beser teaches Unsecure Names / IP addresses of end devices being associated with unique identifiers (such as phone numbers, email addresses, domain name), where this association is made at a third party network device, that provides routing between end devices via the retained list of association. Beser further teaches Secure Names / private IP address of end devices that are packetized so as to translate a packet between end devices where source / destination addresses are of intermediary linking devices (first 14, second 16, trusted third party 30), not the Originating 24 and Terminating 26 devices, who's address is hidden within the packet. (see column 11, line 25 through column 12, line 19, column 10, lines 36-41, and figure 1)

2. Independent Claim 1

a. "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire to Securely Communicate with the First Device"

Patent Owner argues that Claim 1 recites, among other things, "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device" and … "that none of the transmissions [112], [114], or [118] from figure 6 are able to be treated as the "message" as is claimed."

The Third party requester responds that "*the description of Figure 6 in Beser (which is prominently displayed in the Request to illustrate how claim 1 is anticipated) explains that it is "a block-diagram illustrating the message flow* ". Beser at 3:30-32."

"The claims, however, do not delineate how a request must be transported or received, or, for that matter what a "first device" may comprise. They also do not restrict which of several devices in a path of communications may be the "first" or "second"

device. Thus, the telephony, network devices (e.g., edge routers) and/or trusted third party network device described in Beser may, at any particular point, be a "first" or "second" device in the claims. What Patent Owner cannot contest is that Beser shows that messages are sent and received by devices that correspond to the secure name associated with the corresponding device (e.g., the private IP address of the other device). Patent Owner's theory that messages cannot be sent via intervening devices is refuted by its own disclosure, which show analogous deployments to those in Beser. As the '181 patent explains: ",,, a first computer 2401 communicates with a second computer 2402 through two routers 2403 and 2404. Each router is coupled to the other router through three transmission links."

The Examiner agrees with the third party requestor that transmission of messages, albeit through one or more intermediary devices, is still transmission of a message between a “first device” and a “second device”, as claimed. The fact that the ‘181 Patent's disclosure, shows intermediate devices proves the above point, in addition to the fact that in any message communication there is an initiation device and a destination device, where the path a communication travels between the two devices is substantially irrelevant to the fact that the message is being transmitted between end devices, via a path, which may comprise of intermediate routers, servers, or other network communication enabling devices.

b.

Patent Owner argues that “Claim 1 recites both a "first device" and a "second device" that include certain claimed features. For example, claim 1 recites, among other things:

- receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device; and
- sending a message over a secure communication link from the first device to the second device.

Beser does not disclose a "first device" and a "second device" each including all of these features.”

The Third party requester responds that *“Beser cannot be deciphered. In reality, Beser shows a system where the private IP address of a second edge router and/or telephony device is in a message provided to the first router/telephony device. This meets the requirements of the claims. It also is immaterial whether the "first device" is considered to be the telephony device, the edge router or both working together- there is no restriction on the claims to this extent.”*

The Examiner agrees with the third party requestor, the claim merely requires a message, including an IP address, being sent between two devices ("first device"/"second device"). Where the Beser system utilizes an unsecure name (public IP address) to reference another network end, so rather than transmitting a private IP address over the internet, a reference to that end device can be transmitted, and deciphered at an intermediate secure point during transmission, so as to match with the corresponding private IP address, and effect secure communication (see column 11, lines 26 through column 12, line 19).

c.

Patent Owner argues that "*The Office and Requester allege that the tunneling association of Beser corresponds to the claimed "secure communication link" because the "tunneling association hides the identity of the originating and terminating ends of the tunneling association from other users of a public network," and because the broadest reasonable interpretation of a secure communication link does not require encryption. (Req. at 28.) This is incorrect because (1) the broadest reasonable interpretation of secure communication link requires encryption, and Beser's tunneling association is not encrypted;*"

The Third party requester responds that "Instead, Beser consistently and repeatedly points out that encryption in IP tunneling schemes (of which its system is one) is conventional and ordinarily should be used. Beser at col. 1, ll.54-56 ('°Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with [P Security ('IPSec')."') In fact, Beser specifically refers to Kent (the RFC describing the IPSec protocol) to explain how encryption is conventionally incorporated into IP tunneling schemes. Certainly, Beser does indicate that certain applications may raise practical challenges in using encryption in IP tunneling schemes- particularly, "VOIP and multimedia," However, this concern is not an express teaching (as Patent Owner contends)to never use IPSec or other encryption-based IP tunneling models, or that the Beser techniques are an alternative to using encryption-- a conclusion in which the Patent Office expressly agrees. '788 Order at 32. Instead, Beser points out that these practical concerns do not always arise for these two data types, and do not arise at all for data transfer scenarios other than those two types. As Beser explains, even in these two high data volume applications, encryption should generally be used. Beser at col.2, e 11.12-14 (indicating that in a particular VOIP system that uses a VPN, 'the tunneled IP packets, however, may, need to be encrypted., before encapsulation in order to hide the source IP address,")."

The Examiner agrees with the third party requestor as Beser specifically teaches utilization of encryption in combination with the tunneling, where this tunneling is being used as an additional means of making the channel for transmission secure, yet used in combination with legacy encryption to ensure data security (see column 2, lines 1-16).

Patent Owner argues that *"(2) even if the Office determines that a secure communication rink does not require encryption*, *Beser's tunneling association still is not a secure communication link.*"

The Third party requester responds that *“Rather than teaching away from a secure communication link, as Patent Owner contends, "Beser teaches its tunneling invention efficiently solves the problem of encrypted IP packets with readable source addresses." Id As explained in the Request, the inventive tunneling method of Beser "is designed to protect the integrity of the private IP address and ensure the anonymity of the terminating devices." Request at 26, The solution of Beser is thus a distinct layer of security because IPsec encrypted IP packets, for example, cannot conceal the identity of the source addresses. Id. at 26-29; see a/so'788 ACP at 32. Accordingly, "Beser discloses a secure communication link." '788 ACP at 32,””*

The Examiner agrees with the third party requestor as Beser entire patent is dedicated to creating an alternate and/or supplementary to encryption means of securing communication. The method of Beser provides an additional layer of security by not only encrypting data but hiding the source and destination IP addresses (see column 11, line 25 through column 12, line 19).

3. Independent Claim 2

Patent Owner argues that the trusted-third-party network device 30" of Beser does not disclose a "secure name service" because it "omits any description of how the trusted- third-party network device is associated with any form of security." Response at 12-13.

The Third party requester responds that *“Beser teaches that "the end-point devices (24, 26) each have a secure name that comprises a 'unique identifier' that is* *registered with the trusted-third party," and further that the "association of the public [P address for [a network device] with the unique identifier is made on the trusted-third-party network device 30." Request at 32, Further, Patent Owner made representations during the prosecution of the related '180 patent as to the construction of the terms "secure name" and "secure name service," which was noted by the Examiner, Order at 5, In particular, Patent Owner explained that a "'secure name' is a name associated with a network address associated of a [SIC]first device, The name can be registered such that a second device can obtain the network address associate with the first device from a secure name registry and send a message to the first device." Order at 5"*

The Examiner agrees with the third party requestor as Beser's whole inclusion of the third party network device in the path of communication between the first and second devices is for use as a secure name registry that translates the public name for the destination to that actual IP address that had been unused in transmission up until reaching the third party network device to maintain security of destination.

4. Dependent claim 5

Patent Owner argues that "The Office and Requester do not allege that the tunneling association of Beser includes messages that are encrypted. Rather, the Office Action and Request allege that "encryption can be used" because a background portion of Beser references IPSec. (Req. at 36.) First, this limited reference to IPsec is not part of the tunneling association of Beser, (Keromytis Decl. ¶ 34), and thus cannot be used to support a rejection under § 102. See Net MoneyIN, Inc., 88 USPQ2d at 1758. Even so, for reasons similar to those in support of claim 1, Beser discloses IPsec and other encryption techniques only to the extent that they should not be used in tunneled connections and VoIP applications, the technology with which Beser is primarily concerned. (Keromytis Decl. ¶ 34.)"

The Third party requester responds that "Patent Owner's analysis of Beser is incorrect for many of the reasons already stated. Request at 36-37. The Patent Owner also ignores the disclosures in Beser that show that encryption is, in fact, used in the Beser DNS systems. Specifically, Beser teaches that queries involving the unique identifier [e.g,, a domain name] may be encrypted, Beser at col 11, 11:22-25 ("The IP 58 packets may require encryption., or authentication to ensure that the unique identifier cannot be read on the public network 12,"). ,Beser thus clearly teaches that encryption can be used in various ways to support secure communication links (e.g,, use of IPSec-compliant systems, use during negotiation and establishment of the secure communication link)."

The Examiner agrees with the third party requestor, as clearly stated in column 11, lines 22-65, encryption may be used in combination with the tunneling, to ensure that the unique identifier cannot be read on the public network. This encryption is said to be with respect to the "IP packets 58", which includes the "public IP 58 addresses" and "private IP 58 addresses".

6. Dependent claim 6

Patent Owner argues that “the Office and Requester merely allege that "[i]t would be inherent in Beser to ‘decrypt' the very information that it recommends encrypting." (Req. at 37.) This allegation fails because the rejection has not pointed to a single feature in Beser in which decrypting the message would be necessarily present”

The Third party requester responds that “Patent Owner's response is meritless, as it ignores the unambiguous disclosure of the encryption of IP packets in Beser, as discussed repeatedly above, which, to be functional, inherently require decryption of those packets. See also Request at 37"

The Examiner agrees with the third party requestor, as encryption without later decryption makes the data transmitted inoperable, which would not be the intent of the Beser system.

7. Dependent claim 7

Patent Owner argues that “merely reciting a laundry list of standards does not disclose a device "capable of supporting a secure communication link as well as a non-secure communication link," or "establishing a non-secure communication link with the second device when needed," as recited by claim 7.”

The Third party requester responds that “no additional explanation is necessary--claim 7 only requires that the disclosed system be “capable" of supporting a non-secure communication link." Moreover, Beser clearly explains that its preferred embodiment includes devices "that can interact with network system[] based on standards proposed by" IEEE, ITU, IETF, or WAP, for example. Beser at col.4, 11.55-63. Such standards--which were well-known to one skilled in the art prior to February of 2000 --would include those "capable" of supporting non-secure communication links. Second, it is not necessary that Beser incorporate the proposed standards-- all that is necessary is that Beser explains that the disclosed systems are capable of supporting such standards, which Beser has done. Thus, contrary to Patent Owner's assertion"

The Examiner agrees with the third party requestor as Beser has shown communication between the first and second network devices being via standard a such as "IEE, ITU, IETF, or WAP" (see 4:55-63). The fact that the system is "capable" of using each of these standards satisfies the claim.

8. Dependent claim 9

Patent Owner argues that “the Office and Requester have not described what portion of Beser discloses that a secure communication link is enabled, and then initialized "after it is enabled," as recited by claim 9.”

The Third party requester responds that “Beser explains that, in response to a request containing a unique identifier specifying the location of a second network device, the trusted-third-party network device will negotiate with first and second network devices to establish an IP tunnel between the first and second network devices. Beser further explains that the "negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26)." Id. at col. 12, ll.6- 19. The private fretwork IP addresses are then used in conjunction with the public IP addresses of the first and second network devices to establish the tunnel (i.e. the secure communication link) automatically between the first and second network devices. See id. at col.12, ll. 28-37. These steps occur without any interaction from the user that originally made the request. Thus, as the Request explained, the Beser processes are "automatic" and transparent m the user."

The Examiner agrees with the third party requestor, as Beser teaches that the computer system sets up the secure communication (without further user interaction) after initial request to communicate.

9. Dependent claims 10 and 11

Patent Owner argues that "The Office and Requester allege that Beser discloses these features by citing to a portion of Beser that discusses hiding the IP addresses of the originating and terminating devices inside a payload field during negotiation of a tunneling association. (Req. at 38-39, citing Beser 12:6-19.) However, this portion of Beser is directed to what Requester alleges to be the secure communication link, not the alleged "message containing the network address." The Office and Requester also allege that the features of claims 10 and 11 are anticipated because Beser discloses that tunneling "is accomplished by encapsulating the IP packet to be tunneled within the payload field of another packet that is transmitted on the public network." (See, e.g., Req. at 38, quoting Beser 2:9-12.) But this portion of Beser is also not directed to the alleged "message containing the network address.""

The Third party requester responds that "Patent Owner also asserts that the identified 'tunneling" is "not directed to the alleged 'message containing the network address.'" ld These responses simply ignore the contents of Beser, which clearly explains that the disclosed security, measures may be performed through "initiating and maintaining a virtual tunnel." Beser at col.6, ll.58-59, Beser further explains file importance of protecting the negotiation process--which comprises messages "containing the network address associated with the secure name of the device"--from hackers. Request at 38. As one goal of Beser is the protection of the identities of the source addresses, it would be illogical to create the tunneling association only after the VoIP connection has been established. Accordingly, the Examiner's rejection of these claims was proper and should be maintained."

The Examiner agrees with the third party requestor as these features are the hallmark of the Beser Patent which utilizes tunneling to hide the private IP addresses of source and destination devices for the purpose of security in transmission.

10. Dependent claim 18

Patent Owner argues that "The Office and Requester cite to a brief disclosure related to encryption and authentication of the alleged secure name (i.e., unique identifier) as corresponding to this feature. However, Beser does not disclose that encrypting or authenticating the alleged secure name (i.e., the unique identifier) has anything to do with the alleged secure communication link (i.e., tunneling association). (Keromytis Decl. ¶ 36.) Thus, merely disclosing that the unique identifier can be authenticated does not disclose that the tunneling association is an authenticated link."

The Third party requester responds that "The Request explains that the IP 58 packets that comprise the negotiation process "may require encryption and authentication to ensure that the unique identifier cannot be read on the public network." Beser at col. 11, ll.22-24. This is the negotiation process that facilitates the establishment of the secure communication link, and the failure of this authentication step would necessarily preclude the establishment of the secure communication link."

The Examiner agrees with the third party requestor that such a process of agreeing to encrypt data on the communication channel sets up the authenticated link, where data is agreed to be transmitted between the two parties through an intermediate third party device (see column 11, line 25 through column 12, line 19).

11. Dependent claim 23

Patent Owner argues that "Claim 23 recites, among other things, "the secure name of the second device is a secure, non- standard domain name." Beser does not disclose that the unique identifier (referred to as a "domain name") is a "non-standard domain name." (Keromytis Decl. ¶ 37.) Consequently, Beser cannot anticipate claim 23 because "each and every element as set forth in the claim" is not found in Beser."

The Third party requester responds that "Patent Owner is incorrect, as it ignores its own representations of the term "non-standard domain name" during prosecution of the '180 patent. Request at 45; Order at 5. There, the Patent Owner explained that a "'secure name' can be a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number," Id As explained in the Request, the "unique identifier is any of a dial-up number, an electronic mail address, or a domain name." Request at 45."

The Examiner agrees with the third party requestor as any of a dial-up number, an electronic mail address, or a domain name can be used as a secure name to access the device.

12. Independent Claim 24

Patent Owner argues that there is "simply no evidence" that the limitation of 'at the first device requesting and obtaining registration of a secure name for the first device' is necessarily present in Beser to support an inherency theory.

The Third party requester responds that "The Request explains that 'the trusted-third-party network device 30 may be a directory service… that retains a list of E.164 numbers for its subscribers." Request at 46. Such a list is only possible if the devices request and obtain registration of their respective secure names. Patent Owner presents no other response to the rejection of claim 24 with respect to any of its other limitations and instead relies on those allegations "similar to those given in support of the patentability of claim 1." Because the rejection of claim 1 was proper, the rejection of claim 24 based on Beser should be maintained.

The Examiner agrees with the third party requestor as Beser has maintains a director server (service) that allows devices to register secure names for their respective devices.

12. Claims 25-29

With respect to claims 25-29, Patent Owner presents no distinct responses from those offered in the claims previously discussed above. Because the rejections of those claims were proper, the rejection of claims 25-29 based on Beser were also proper and should also be maintained.

Dependent claims 3-4, 8, 12, 14-15, 17, and 19-22 (no arguments presented)

C. Rejections Under Mattaway (ISSUE 3)

1. Overview

Mattaway teaches a connection server 26 that maintains a database 34 of callee email addresses and associated IP addresses, so that when a request is made for a connection via a caller, the caller can be connected to the callee via the association stored at the server. (see column 7, lines 20-36)

2. Independent Claim 1

a.

Patent Owner argues that “First, Mattaway does not disclose that the email address in Table 9 is associated with any particular device, much less the alleged "callee's device" or any other device allegedly associated with the claimed "first device." (Keromytis Deck ¶ 44.) Mattaway discloses that the data in Table 9 (including the alleged secure name) is returned to a user (i.e., the caller in the cited example) in response to a user "logging on for the first time" to a global server. (Mattaway Fig. 17A, 22:65- 23:2.) The email address described in Table 9 is not referenced in any other portion of Mattaway, and Mattaway is completely silent as to the function of the referenced email address and whether it could be associated with a device. (Keromytis Decl. ¶ 44.)”

The Third party requester responds that “Mattaway explains that the data in Table 9--which includes the encrypted email address "eemailAddr" entry--is used by global server 1500 "'in the event that the WebPhone client process is logging on for the first time" in order to register certain information from that particular new WebPhone client. Mattaway at col.22, ll.65-59. Mattaway thus discloses that information requested from the first device/WebPhone client would include an encrypted email address.”

The Examiner agrees with the third party requestor as Mattaway specifically teaches, in column 7, lines 25-37 IP addresses being found utilizing email addresses at the connection server.

Patent Owner argues that “Second, the firewall of Mattaway does not protect email addresses as alleged by the Office and Requester. (Keromytis Decl. ¶ 45.) In fact, if a callee's email address were to be stored on a server behind the firewall (e.g., the global server 1500), that email address would already be known to the caller before the caller connects to the server. ”

The Third party requester responds that Patent Owner attempts to read non-existent limitations into a "secure name" and its representations now are inconsistent with those it made during prosecution when it told the Patent Office this term was not so limited. Indeed, before the Patent Office, the Patent Owner represented that the claimed "secure name" could be as simple as a telephone number, Order at 5, which undoubtedly "would already be known by the caller." Accordingly, Mattaway discloses "a first device associated with a secure name and an unsecured name." The Examiner's rejection was proper and should be maintained.

The Examiner agrees with the third party requestor as in Mattaway, a user may use an alias to access the secured data protected under the firewall, where the secured data includes email addresses and IP addressed (see column 4, lines 50-54 and column 17, lines 44-54). Mattaway further shows the email addresses being encrypted email addresses (see 40:27).

Patent Owner argues that “Third, nothing in Mattaway discloses or suggests that an email address received by the global server of Mattaway, or used by the caller or callee, is a "secure name," much less associated with any security whatsoever. (Keromytis Decl. ¶ 46.) In fact, the terms "secure" or "security," or the like, are completely absent from Mattaway.”

The Third party requester responds that, again, “the Patent Owner represented that the claimed "secure name" could be as simple as a telephone number, Order at 5, which undoubtedly "would already be known by the caller." Accordingly, Mattaway discloses "a first device associated with a secure name and an unsecured name.""

The Examiner agrees with the third party requestor as in Mattaway, a user may use an alias to access the secured data protected under the firewall, where the secured data includes email addresses and IP addressed (see column 4, lines 50-54 and column 17, lines 44-54). Mattaway further shows the email addresses being encrypted email addresses (see 40:27).

b.

Patent Owner argues that Mattaway doesn’t teach "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device."

The Third party requester responds that “the second device retrieves the "network address corresponding to the secure name associated with the first device" from the connection server. Request at 70. The Request also explained that after receiving the IP address of the first device, the second device may "directly establish the point-to-point Internet communications with the [first device] using the IP address of the [first device]." Request at 72. Mattaway discloses these "point-to-point Interact communications" are accomplished by the second device "'open[ing] up a socket" to the first device. See Mattaway at col.24, ll.l5-30. The second device transmits a " " packet to the first device, to which the first device may, among other things, acknowledge or reject the call, Mattaway at col.24, l.11 - col.25, l.12. This process "enables the parties to converse in real-time, telephone quality, encrypted communication over the Interact and other TCP/IP based networks." Mattaway at col.25, ll.32-34."

The Examiner agrees with the third party requestor as the process described in column 24, line 11 through column 25, line 34, explains the callee receiving a request to communicated from the caller, to which the callee can either <REJECT>, or accept (<CALL ACK>) the call thereby establishing the connection.

c.

Patent Owner argues that Mattaway fails to disclose "Sending a Message Over a Secure Communication Link from the First Device to the Second Device."

The Third party requester responds that "Patent Ovmer's assertion is frivolous. The literal distance within the pages of the patent between these two cites is irrelevant--the disclosure of "encrypted communications" in Mattaway follows a detailed explanation of the operation of the WebPhone client and is hardly a miscellaneous feature. See also Request at 72."

The Examiner agrees with the third party requestor as previously discussed once the callee accepts the call, "the WebPhone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks"

3. Independent Claim 2

Patent Owner argues that Mattaway lacks teaching of " "from a first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device." The Office and Requester fail to show disclosure of a "secure name service" because, as indicated above, the alleged secure name service (i. e., connection server 26) does not store a "secure name" for the callee's device, as proposed by the Office and Requester."

Patent Owner attempts to read non-existent limitations into a "secure name" and its representations now are inconsistent with those it made during prosecution when it told the Patent Office this term was not so limited. Indeed, before the Patent Office, the Patent Owner represented that the claimed "secure name" could be as simple as a telephone number, Order at 5, which undoubtedly "would already be known by the caller." Accordingly, Mattaway discloses "a first device associated with a secure name and an unsecured name." The Examiner's rejection was proper and should be maintained.

The Examiner agrees with the third party requestor as in Mattaway, a user may use an alias to access the secured data protected under the firewall, where the secured data includes email addresses and IP addressed (see column 4, lines 50-54 and column 17, lines 44-54). Mattaway further shows the email addresses being encrypted email addresses (see 40:27).

4. Dependent Claims 6-9, 12-17, and 19-21

No new argument presented under this heading.

5. Dependent Claim 6

Patent Owner argues that claim 6 should not be rejected as claim 5 from which it depends was not rejected under issue 3.

The Examiner agrees with the Patent Owner, as this was a typographical error that has since been corrected.

6. Dependent Claim 7

Patent Owner argues that “merely reciting a few example protocol names does not disclose a device "capable of supporting a secure communication link as well as a non-secure communication link," or "establishing a non-secure communication link with the second device when needed," as recited by claim 7. (Keromytis Decl. ¶ 50.) Consequently, the rejection of claim 7 cannot be sustained. Besides, Mattaway does not disclose how the named protocols could be used to effectuate the claimed feature, (id.), and neither of the purported "protocols" have properly been incorporated by reference into Mattaway so as to provide sufficient support for a rejection.”

The Third party requester responds that “capable of interacting with "datagram services such as Interact Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) on top of the IP." Request at 75, Patent Owner responds only that an additional explanation is needed "to effectuate the claimed feature" and that the protocols identified in Mattaway have not "properly been incorporated by reference." Response at 23-24. First, no additional explanation is necessary--the claim only requires that the disclosed system be "capable" of supporting a non- secure communication link. Mattaway clearly explains that its devices are accessible through a number of protocols including IP, TCP, RLP and UDP. Request at 75. Such protocols--which were well-known to one skilled in the art--would include those "capable" of supporting such non- secure communication links. Second, it is not necessary that Beser incorporate those protocols--- 'all that is necessary is that it explains that the disclosed systems are capable of supporting the protocols, which Mattaway has done, Thus, Mattaway discloses a system that anticipates claim 7, and the Examiner's rejection was proper and should be maintained."

The Examiner agrees with the third party requestor as the claim merely recited a capability to support non-secure data channels where Mattaway lists channels that may support non-secure communication links.

Dependent Claim 9

Patent Owner argues that Claim 9 recites, among other things, "automatically initiating the secure communication link after it is enabled." The Office and Requester assert that the alleged secure communication link would be established automatically because "nothing in the specification [of Mattaway] suggests user interaction is involved regarding the underlying actions of the computer programs that set up the... communications." (Req. at 76.) Hence, the Office and Requester allege that the claimed feature is disclosed by Mattaway merely because Mattaway omits something that may challenge the presence of the feature. This type of allegation does not indicate to Patent Owner where "each and every element as set forth in the claim" is disclosed, Verdegaal Bros., 814 F.2d at 631, and cannot be a basis for a prima facie case of anticipation. See 35 U.S.C. § 132. Moreover, the Office has not described what portion of Mattaway discloses that a secure communication link is enabled, and then initialized "after it is enabled," as recited by claim 9. See Net MoneyIN, Inc., 88 USPQ2d at 1758 (anticipation requires "all of the limitations arranged or combined in the same way as recited in the claim"). For these reasons, the rejection of claim 9 is deficient and should be withdrawn.

The Third party requester responds that “Patent Owner is apparently relying on the putative absence of the terms "automatically initiating" in Mattaway to assert that the disclosed initiation of a secure communication link between two WebPhone clients would not occur automatically. As explained in the Request, Mattaway describes computer processes that are transparent to the user and thus, within the broadest reasonable scope of the claim term "automatic." Request at 76. As Mattaway explains, in response to the return of an "Internet Protocol address of the callee from the global server 1500, the packet transmission sequence illustrated between WebPhones 1536 and 1538 of FIG. 17A transpires." Mattaway at col.24, ll.11-14. This step occurs without any interactions by the user that originally made the request. Consequently, the Examiner's rejection of claim 9 was proper."

The Examiner agrees with the third party requestor as Mattaway discloses in col.24, ll.11-14, that once the call is requested initiation of the secure channel (or socket) is automatically effected by the system.

8. Dependent Claim 13

Patent Owner argues that Claim 13 recites, among other things, "wherein the receiving and sending of messages through the secure communication link includes multiple sessions." The Office and Requester allege that this feature is disclosed because "each call, i.e., session, 'may be assigned a successive session number...'." (Req. at 76, quoting Mattaway 6:24-36.) However, Mattaway discloses that each call receives a new session. (Mattaway 6:24-36; Keromytis Decl. ¶ 51.) Since the Office and Requester have taken the position that "point-to-point Internet communications with the callee" that arise from a single call correspond to the claimed secure communication link, (Req. at 74), the Office and Requester cannot now allege that the alleged communication link has more than one session. See Net MoneyIN, Inc., 88 USPQ2d at 1758. Consequently, the alleged secure communication link does not include "multiple sessions," as recited by claim 13. (Keromytis Decl. ¶ 51 .)

The Third party requester responds that "Mattaway cannot disclose this limitation because "each call receives a new session" and Requester has taken the position that a "single call" corresponds to the claimed secure communication link. Patent Owner is incorrect. Request at 76. Initially, Requester did not assert that a "single call" corresponds to the claimed secure communication link. As explained in the Request, the encrypted point-to-point communication link between two WebPhone clients comprises the claimed "secure communication link," not an individual session. Request at 74. And, as Mattaway explains that each successive call between a given pair of WebPhone clients would be assigned a "successive session number,""

The Examiner agrees with the third party requestor as Mattaway points out in column 25, lines 13-23 a "previously opened socket" being used for further communication where each session has a unique "session ID number".

9. Dependent Claims 14 and 15

Patent Owner argues that Claim 14 recites, among other things, "supporting a plurality of services over the secure communication link." The Office and Requester allege that this feature is disclosed by the naming of two example datagram services that may be used in establishing communication with a callee processing unit. (Req. at 77, citing Mattaway 6:37-45.) However, the mere recitation of a few alternative names does not disclose the claimed "supporting a plurality of services over a secure communication link." Mattaway also does not disclose how the named "protocols" could be supported or used to effectuate the claimed feature, and neither of the purported "protocols" have properly been incorporated by reference into Mattaway as to provide sufficient support for a rejection under § 102(e). See AdvancedDisplay Sys., Inc., 212 F.3d at 1282. The Office and Requester further allege that Mattaway discloses a "plurality of application programs" and points to a single "WEBPHONE" program that may be executed on a machine that runs one of several operating systems. (Req. at 77, citing Mattaway 4:38-41.) **However, disclosure of a single program that may be run on various alternative operating systems does not disclose, or even relate to, supporting a plurality of services over a secure communication link.** Consequently, the rejection of claim 14 under § 102 cannot be sustained. Claim 15 recites, inter alia, "the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof." Claim 15 is dependent from claim 14, includes all the limitations of claim 15, and is patentable for reasons similar to claim 14. Accordingly, the rejection of claims 14 and 15 under § 102(e) should be withdrawn, and the patentability of claims 14 and 15 be confirmed.

The Third party requester responds that “Mattaway shows that the disclosed protocol-based system that includes networked devices that support "datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) on top of the IP." Request at 77. Patent Owner responds only that "additional explanation" is needed "to effectuate the claimed feature" and that the protocols identified in Mattaway have not "properly been incorporated by reference," Response at 25. No "additional explanation" is necessary - the claim only specifies "supporting a plurality" of services over the secure communication link." Request at 77, Mattawav also explains its devices are accessible through a number of protocols including IP, TCP, RTP and UDP. Request at 75. Such protocols--which would be well-known to one skilled in the art--would include those capable of supporting non- secure communication links. Second, it is not necessary that Beser incorporate those protocols-- all that is necessary is that it explains that the disclosed systems are capable of supporting them, which Mattaway has done. Further, as explained in the Request, Mattaway also discloses the application program "WEBPHONE® Internet Telephony application," may be utilized for either audio via the UDP protocol or video using UDP and RTP Protocols. Given the breadth of the term "services" as indicated by claim 15, it is clear that Mattaway supports a plurality of "services" over the secure communication link, thus, contrary to Patent Owner's assertion, Mattaway discloses a system that anticipates claim 14. Consequently, the Examiner's proposed rejection of claim 14 was proper and should be maintained, Patent Owner presents no distinct response to the rejection of claim 15 based on Mattaway relative to its response to the rejection of claim l4. Accordingly, for the reasons noted above, the Examiner's rejection of claim 15 based on Mattaway was also proper and should be maintained."

The Examiner agrees with the third party requestor as Mattaway uses the "WEBPHONE® Internet Telephony application," for either audio via the UDP protocol or video using UDP and RTP Protocols, the reference is shown to support different services being rendered via various protocols.

10. Independent Claim 24

Patent Owner argues that Claim 24 recites, among other things, "at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address." The Office and Requester assert that Mattaway discloses this feature because Mattaway discloses "the first processing unit 12 automatically transmits its associated E-mail address ... to the connection server 26." (Req. at 80-81, quoting Mattaway 6:60-65.) For at least the explanations similar to those described above regarding independent claim 1, Mattaway does not disclose or suggest a "secure name." Moreover, automatically transmitting an email address does not evidence disclosure of "requesting and obtaining registration" of the email address, much less of a "secure name." (Keromytis Decl. ¶ 52.) The Office and Requester have also not articulated what in Mattaway corresponds to "requesting" and what in Mattaway corresponds to "obtaining," or how it takes place "at the first device." See 35 U.S.C. § 132. Claim 24 also recites "receiving at the network address associated with the secure name of the first device a message from a second device of the desired to securely communicate with the first device." The allegations that this feature is disclosed by Mattaway are substantially identical to those given in the rejection of claim 1, (compare Req. at 70-71 with id. at 81-83), and Mattaway does not disclose this feature for reasons similar to those given in support of patentability of claim 1. Claim 24 further recites "sending a message securely from the first device to the second device." The Office and Requester allege that this feature is disclosed by a brief, isolated passage in Mattaway reciting that a "WebPhone application enables the parties to converse in real-time, telephone quality, encrypted audio communication." (Req. at 83, quoting Mattaway 25:32-34.) However, this passage discloses nothing about whether, much less how, a message may be sent securely, (Keromytis Decl. ¶ 54), and therefore does not meet the level of disclosure required to show anticipation of claim 24. See Net MoneylN, Inc., 88 USPQ2d at 1758. In particular, this passage does not disclose at least "sending a message securely from the first device to the second device." Accordingly, the rejection of claim 24 should be withdrawn.

The Third party requester responds that “the only new argument presented by Patent Owner is that there is no evidence of "requesting and obtaining registration." Response at 24-25. Patent Owner simply ignores the disclosures in Mattaway describing the registration of the secure name at the connection server by a first user upon initiating the "point-to-point Internet protocol," Request at 80. For example, Mattaway explains that "in the event that the WebPhone client process is logging on for the first time, global server 1500 returns to the WebPhone 1536 a packet .... In response, WebPhone 1536 returns a packet" that is used by the connection server to "update database 1516." Mattaway at col.22, l.65 - col.23, l.8. A " packet ... that enables certain functions within the WebPhone" is then transmitted from the global server. Mattaway at col.23, ll.5-19. Thus, Mattaway plainly shows "requesting and obtaining registration." Patent Owner presents no response to the other limitations in claim 24, but simply relies on assertions made as to other claims. Because the rejections of those other claims were proper, the rejection of claim 24 based on Mattaway should be maintained."

The Examiner agrees with the third party requestor as when a user logs on for a first time the user is automatically registered with the server, upon subsequent log on request by the user, the user is registered with the system and their corresponding status is changed to an online state (see 22:65 through 23:37).

11. Dependent Claim 25

Patent Owner argues that Claim 25 recites, among other things, "wherein sending a message securely comprises sending the message from the first device to the second deice using a secure communication link." The allegation that this feature is disclosed by Mattaway is substantially identical to that given in the rejection of claim 1, (compare Req. at 30-31 with id. at 50-50), and therefore claim 25 is patentable for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 25 should be withdrawn.

The Third party requester responds that "Patent Owner presents no distinct response from those offered for other claims. Because the rejections of those other claims were proper, the rejection of claim 25 based on Mattaway should also be maintained. See also Request at 83."

The Examiner agrees with the third party requestor.

12. Independent Claim 26

Patent Owner argues that Claim 26 recites, among other things, "from the first device requesting and obtaining registration of an unsecured name associated with the first device." The Office and Requester on Mattaway's disclosure that a "party's name may be stored in a 'personal information directory.'" (Req. at 85.) However, the personal information directory of Mattaway is located on what the Office and Requester point to as the first device, (see Req. 84-85), and the Office and Requester do not explain how an "alias" or "party's name" stored on the first device evidences disclosure of the claimed feature of "from the first device requesting and obtaining registration of an unsecured name associated with the first device." Assuming for the sake of argument that the "alias" or "party's name" could be stored on a device different from what the Office and Requester point to as the first device, the Office and Requester still cannot evidence disclosure of "requesting and obtaining registration of an unsecured name associated with the first device." The Office and Requester have not even articulated what in Mattaway corresponds to the claimed "requesting," or what corresponds to the claimed "obtaining." Indeed, a review of Mattaway reveals that at least these features are not disclosed at all. Consequently, the rejection of claim 26 should be withdrawn. Claim 26 also recites, "from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device." For at least the explanations similar to those described above regarding independent claim 1, Mattaway does not disclose or suggest a "secure name." Even so, automatically transmitting an email address, even if that email address is subsequently stored in a database, does not evidence disclosure of "requesting and obtaining registration" of that email address, much less a "secure name." The Office and Requester have not articulated what in Mattaway corresponds to "requesting" and what in Mattaway corresponds to "obtaining." See 35 U.S.C. § 132. Claim 26 further recites, "receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device," and "from the first device sending a message securely from the first device to the second device." The allegations that these features are disclosed by Mattaway are substantially identical to those given in the rejection of claim 24, (compare Req. at 81-83 with id. at 85-87), and Mattaway does not disclose this feature for reasons similar to those given in support of patentability of claim 24. Accordingly, the rejection of claim 26 should be withdrawn.

The Third party requester responds that “Patent Owner's response attempts to read non-existent limitations into the claims - neither the claims nor the specification disclose the claimed step of "requesting and obtaining registration of an unsecured name" from occurring solely on the first device. In fact, the term "unsecured name" appears nowhere in the specification Patent Owner's contentions on the implied meaning of this term, thus are made of whole cloth. Because Patent Owner presents no other response to the rejection of claim 26 other than those presented in response to rejections of other claims, and because those other rejections were proper, the rejection of claim 26 "based on Mattaway… as proper and should be maintained.”

The Examiner agrees with the third party requestor.

13. Dependent Claim 27

Patent Owner argues that Claim 27 depends from claim 26, includes all of its features, and is patentable for at least the reasons discussed above for claim 26. Accordingly, the rejection of claim 27 should be withdrawn.

The Third party requester responds that “Patent Owner presents no distinct responses from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claims 27-29 based on Mattaway were also proper and should be maintained.”

The Examiner agrees with the third party requestor.

14. Independent Claim 28

Patent Owner argues that Claim 28 recites, among other things, "sending a message to a secure name service, the message requesting a network address associated with a secure name of a device." The Office and Requester do not specify how Mattaway discloses the claimed "secure name of a device" or "secure name service," and, for that reason alone, the rejection of claim 28 is deficient and should be withdrawn. Even so, Mattaway does not disclose a "secure name of a device" at least for reasons similar to those given in support of patentability of claim 1, and does not disclose the feature of "a secure name service" at least for reasons similar to those given in support of patentability of claim 2. Claim 28 also recites, "sending a message to the network address associated with the secure name of the device using a secure communication link." The allegation that this feature is disclosed by Mattaway is similar to that given for the "secure communication link" of claim 1, (compare Req. at 72 with id. at 90), and Mattaway does not disclose this feature for reasons similar to those given in support of patentability of claim 1. Accordingly, the rejection of claim 28 should be withdrawn.

The Third party requester responds that “Patent Owner presents no distinct responses from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claims 27-29 based on Mattaway were also proper and should be maintained.”

The Examiner agrees with the third party requestor.

15. Independent Claim 29

Patent Owner argues that Claim 29 recites, among other things, "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desire to securely communicate with the first device, wherein the secure name of the first device is registered." The allegation that this feature is disclosed by Mattaway is substantially identical to that given in the rejection of claim 1, (compare Req. at 70-71 with id. at 92-94), and Mattaway does not disclose this feature for reasons similar to those given in support of patentability of claim 1.

Additionally, the Office and Requester do not specify how Mattaway discloses "wherein the secure name of the first device is registered," and, for that reason alone, the rejection of claim 29 is deficient and should be withdrawn. See 35 U.S.C. § 132. Claim 29 further recites, "sending a message securely from the first device to the second device." The allegation that this feature is disclosed by Mattaway is substantially identical to that given in the rejection of claim 24, (compare Req. at 83 with id. at 94), and Mattaway does not disclose this feature for reasons similar to those given in support of patentability of claim 24. Accordingly, the rejection of claim 29 should be withdrawn. For at least the reasons discussed above, all anticipation rejections based on Mattaway should be withdrawn and claims 1, 2, 6-9, 12-17, 19-21, and 24-29 should be confirmed.

The Third party requester responds that “Patent Owner presents no distinct responses from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claims 27-29 based on Mattaway were also proper and should be maintained.”

The Examiner agrees with the third party requestor.

Dependent Claims 8, 12, 16-17, and 19-21

Patent Owner provides no further arguments regarding these claims.

D. Mattaway in view of Beser (ISSUE 4)

Dependent Claims 3 and 4

Patent Owner argues that “Claims 3 and 4 depend from claim 2, so they include all of claim 2's features. The Office and Requester do not allege that Beser makes up for the deficiencies noted above regarding Mattaway's disclosure, (see Req. at 95-96), so claims 3 and 4 are patentable over Mattaway and Beser, alone or in combination, for at least the reasons discussed above regarding claim 2.”

The Third party requester responds that Patent Owner asserts only that "Beser does not make up for the deficiencies noted above regarding Mattaway's disclosure." Response at 28-29, Because the Patent Owner presents no distinct response from that offered in response to the rejection of claim 2 based on Mattaway, the rejection of claims 3 and 4 was proper and should also be maintained. See also Request at 94-95.

The Examiner agrees with the third party requestor.

Dependent Claims 10 and 11

Patent Owner argues that “As explained in support of claim 1, however, the Office and Requester do not explain what an "encrypted audio communication" is or how it allegedly discloses the claimed features.”

The Third party requester responds that this argument is answered above.

The Examiner agrees with the third party requestor.

Patent Owner argues that “With regard to claim 2, from which this claim depends, the Office and Requester allege that Mattaway discloses the feature of a "message containing the network address" because connection server 26 sends an IP address of the caller to the first processing unit 12, (Req. at 74, citing Mattaway 7:32-37), and that Beser also discloses the feature because Beser states "the first network device (14) has the following network addresses . . . ," (Req. at 35, citing Beser 21:38-43). Neither of these alleged "messages," however, are received through the alleged "secure communication link" in the respective references. “

The Third party requester responds that this argument is answered above.

The Examiner agrees with the third party requestor.

Patent Owner argues that “The Office and Requester simply have not explained how or why one of ordinary skill in the art would have incorporated Beser's alleged tunneling mechanism into Mattaway's system.”

The Third party requester responds that “The Request explains that a person of ordinary skill in the art would have found motivation within Mattaway to modify the encrypted communications disclosed therein to incorporate additional mechanisms to add additional layers of protection to the secure communication link. Request at 96-97. That person would have found that each of Beser and RFC 2401 identify the same problem (improving security of networked communications) and provide a solution to that problem; namely, use of a particular type of tunneling. In response, Patent Owner asserts no arguments that are distinct from those already advanced with respect to claims 1 and 2. Accordingly, because the rejection of those claims was proper, the rejection of claims 10 and 11 as obvious was also proper and should be maintained."

The Examiner agrees with the third party requestor that an additional layer of security in a system designed to provide security would be an obvious combination.

Dependent Claim 18

Patent Owner argues that "Beser does not explain that encrypting or authenticating the alleged secure name (i. e., the unique identifier) has anything to do with the alleged secure communication link (i. e., tunneling association) in Beser, and therefore it cannot be combined with the alleged secure communication link of Mattaway. (Keromytis Decl. ¶ 56.)"

The Third party requester responds that "The Request \ explains that the IP 58 packets that comprise the negotiation process "may require encryption and authentication to ensure that the unique identifier cannot be read on the public network." Beser at col. 11, 11.22-24. As explained above, it is the negotiation process of Beser, like Mattaway, that facilitates the establishment of the secure communication link. A failure of the authentication described in Beser would necessarily preclude the establishment of the secure communication link. Patent Owner's comments thus rest on an assumption that is technically incorrect. Further, as explained in the Request, a person of ordinary skill in the art would have found motivation within Mattaway to modify the negotiation process disclosed therein to incorporate additional mechanisms to add another layer of protection to establishing the secure communication link. Request at 97-98. That person would find in Beser identification of the same problem (improving security of networked communications) as well as a solution to the same problem, namely, authenticating the secure communication link. Accordingly, the Examiner's rejection of claim 18 was proper and should be maintained"

The Examiner agrees with the third party requestor, and further notes that both public IP address (phone number, email address, domain name, etc.) and private IP address are taught as being encrypted in column 11, lines 18-65 of Beser.

Dependent Claim 23

Patent Owner argues that Beser, however, does not disclose a secure, non-standard domain name for the reasons similar to those discussed above with regard to the rejection of claim 23 under § 102(e) in view of Beser. (See Section III.B. 11; see also Keromytis Decl. ¶ 37.)

The Third party requester responds that "Patent Owner presents no distinct response from those offered in other claims. Because the rejections of those other claims were proper, the rejection of claim 23 based on Mattaway in view of Beser should also be maintained. See also Request at 95-97"

The Examiner agrees with the third party requestor.

E. Mattaway in view of RFC 2401 (ISSUE 5)

Patent Owner argues that “with regard to claim 2, the Office and Requester allege that the claimed "message containing the network address" corresponds to the connection server of Mattaway sending an IP address to the first processing unit 12, and the claimed "secure communication link" corresponds to "point-to-point Internet communications" between first processing unit 12 and a callee. (See Req. at 74.) Given this interpretation, the alleged message is not received through the alleged "secure communication link." RFC 2401 is directed to IPsec, a suite of security protocols, and therefore does not remedy the deficiencies of Mattaway.”

The Third party requester responds that “The Request explains that a person of ordinary skill in the art would have found motivation within Mattaway to modify the encrypted communications disclosed therein to incorporate additional mechanisms to add additional layers of protection to the secure communication link. Request at 96-97. That person would have found that each of Beser and RFC 2401 identify the same problem (improving security of networked communications) and provide a solution to that problem; namely, use of a particular type of tunneling. In response, Patent Owner asserts no arguments that are distinct from those already advanced with respect to claims 1 and 2. Accordingly, because the rejection of those claims was proper, the rejection of claims 10 and 11 as obvious was also proper and should be maintained.”

The Examiner agrees with the third party requestor that an additional layer of security in a system designed to provide security would be an obvious combination.

F. Lendenmann (ISSUE 6)

1. Overview

Lendenmann teaches a Cell Directory Service (CDS) that stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource. (see page 21) Where the client can utilize the namespace maintained by the CDS for the location of a server that handles the interface that the client is interested in (see page 182). Lendenmann further teaches the DCE Naming Service that allows user to identify, by name, resources such as servers, files, disks, or print queues, and gain access to them without needing to know where they are located in a network. (see page 22) Lendenmann further allows for cell name aliasing so as to have a primary name, and one or more alias names that is recognized by DCE services (see page 24). This dual name scheme in Lendenamann provides two naming schemes:

- CCITT X.500 [secure]
- Intemet Domain Name Service (DNS) [not secure]

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." An example of an X.500 name is: [Cell name] [CDS name]. (see page 23)

2. Independent Claim 1

a.

Patent Owner argues that “Lendenmann simply presents X.500 and DNS as two alternative DCE- compatible general naming schemes for organizing network addresses: "X.500 is an emerging global directory service standard, but the Internet domain name system (DNS) is an established industry standard. For interoperability purposes, GDS supports both X.500 and DNS transparently." (Lendenmann 21 .) The Requester attempts to support its assertions by highlighting two differences between the DNS and X.500 schemes, but it fails to explain how these differences suffice to make X.500 "secure" and DNS "unsecured." (Req. at 105.)”

The Third party requester responds that “During prosecution of the '181 patent, the Patent Owner explained that a "secure name" is registered in a "secure name registry" and can include a "secure domain name" but can be as basic as a "telephone number." Order at 5. Further, in a related patent reexamination, the Patent Owner explained that "a conventional domain name service cannot resolve a secure domain name." ld Thus, under its broadest reasonable construction, a "secure name" is defined both by storage in a "secure name registry," and by the fact that it cannot be resolved by a conventional domain name service. A telephone number, according to Patent Owner, would satisfy this definition. Order at 5. Accordingly, as explained in the Request, the CCITT X.500 naming scheme of the DCE environment "is a secure, internal naming convention." Request at 105. The CDS, a directory service component that controls the secure name of a given DCE cell, is integrated into the security server of the CCITT X.500 system and will only complete an operation "if the user is authenticated and authorized." Request at 104. Alternatively, each DCE cell is also represented in the public Internet DNS system with an unsecured name, e.g., a publicly accessible address that may be resolved by a conventional DNS server. Consequently, Lendenmann discloses "a first device associated with a secure name and an unsecured name.""

The Examiner agrees with the third party requestor that the X.500 satisfies the requirement for a secure name, as the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address. Conversely, the if an Internet Address alone is used then a traditional DNS us used to access, leaving the address unsecured and out in the open.

Patent Owner argues that "regardless of whether a user attempts to obtain a network address based on an X.500 name or a DNS name, a user cannot access the CDS at all unless the user is first cleared by the Security Service. (Lendenmann 34; Keromytis Decl. ¶ 63.) The Security Service thus weeds out unauthorized users without regard to the naming scheme employed by each user (X.500 or DNS). (Lendenmann 34; Keromytis Decl. ¶ 63.) Lendenmann does not provide for any second layer of protection in its CDS directory service, and certainly does not disclose any such additional layer of protection based on naming scheme. (Keromytis Decl. ¶ 63.) Nor does the Requester assert that it does. (See Req. at 102-06.) The Requester's strained argument to read "secure" and "unsecured" naming features into Lendenmann therefore fails."

The Third party requester responds as provided above.

The Examiner further submits that as with any network communication there are levels of security where Lendenmann shows a more secure method and a less secure method.

b.

Patent Owner argues that “Even if one were to incorrectly assume that an X.500 name corresponds to a "secure name," the Requester does not identify any passage in Lendenmann describing receiving any message at a network address corresponding to an X.500 name instead of a DNS name. (Keromytis Decl. ¶ 65.)”

The Third party requester responds that “Patent Owner has represented that a "secure name" is defined by where it stored and whether it may resolved by a conventional name server. The CDS of Lendenmann is the directory component that controls names and addresses within a DCE Ceil. A DCE Cell may have both an X.500 name and a DNS name. Request at 106-07. Second, as explained in the Request, Lendenmann explains that "P, PC runtime then directly calls the server process listening to the endpoint." Request at 108 (emphasis added). Upon establishment of an "authenticated RPC," the client can "specify the level of protection to be applied to its communication with the server. The protect level determines the degree to which client/server messages are actually encrypted." Request at 108. Thus, Lendenmann plainly shows the message from the second device indicating a "desire" to securely communicate with the first device. Accordingly, the Examiner's rejection of claim 1 was proper and should be maintained.”

The Examiner agrees with the third party requestor that upon an establishment of a means to secure communication information is transmitted as messages between the two nodes (further see page 29 of Lendenmann)

2. Independent claim 2

a.

Patent Owner argues that “Independent claim 2 recites, among other things "[a] method of using a first device to communicate with a second device having a secure name" (emphasis added). Lendenmann does not disclose this feature because, as discussed above regarding claim 1, Lendenmann does not disclose any "secure" names. Thus, Lendenmann does not anticipate claim 2.”

The Third party requester responded to this argument above

The Examiner agrees with the third party requestor.

b.

Patent Owner argues that “The CDS is not a "secure name service" because it has no bearing whatsoever on whether the communications for which it provides network addresses are secure or not. (Keromytis Decl. ¶¶ 66- 67.) As disclosed and claimed in the '181 patent, a "secure name service" is a service that both resolves a secure name into a network address and further supports establishing a secure communication link. (Keromytis Decl. ¶ 66.)”

The Third party requester responds that “Patent Owner's response should be disregarded because it attempts to read non-existent limitations into the term "secure name service."4 As the Patent Owner has represented to the PTO, a "secure domain name service can resolve addresses for as secure domain name," Order at 5, and a "'secure name' is a name associated with a network address associated [with] a first device" and "can be a secure non-standard domain name" or as basic as "a telephone number." Order at 5. That the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name." Because the X.500 cell naming convention meets these requirements, the CDS is a ”secure name service."”

The Examiner agrees with the third party requestor that as when the CDS (or GDS) is given a X.500 name it returns the network address of the named resource (see page 21), this is opposed to when provided with an Internet Domain Name that is tied directly to internet locations.

c.

Patent Owner argues that “Lendenmann's binding process does not disclose "requesting a network address" associated with any server name at all, let alone a "secure" name. (Keromytis Decl. ¶ 68.) Although Lendenmann generically describes that its CDS may return a network address upon receiving a name, (Lendenmann 21), this does not apply to interactions between a client and the CDS during the binding process.”

The Third party requester responds that “no third party interpretation of Lendenmann is needed here - it expressly discloses the features required by the claims via its description of the DCE system--including "requesting a network address associated with the secure name" and "receiving a message containing the network address associated with the secure name. Request at 111-114. Moreover, that these features may be optionally implemented within the DCE system does not mean Lendenmann does not disclose a system that comprises those features.”

The Examiner agrees with the third party requestor and further elaborates that when a client uses a X.500 name to securely transmit a request while hiding the destination location, the message is forwarded to the CDS (or GDS), which returns the network address of the named resource (see page 21).

d.

Patent Owner argues that “For establishing RPCs, Lendenmann explains that server network addresses are contained in "binding handles." (Lendenmann 182-84, "Network address.") As discussed above, Lendenmann describes its binding process as not returning any particular network address based on a server name, but rather searching for compatible servers and returning binding handles for "several compatible servers." (See Lendenmann 182, 185; Keromytis Decl. ¶ 68.) Thus, for the reasons discussed above, Lendenmann neither discloses "sending . . . the message requesting a network address associated with the secure name of the second device," nor "receiving a message containing the network address associated with the secure name of the second device," and therefore the rejection of claim 2 should be withdrawn, and its patentability confirmed."

The Third party requester responds that "no third party interpretation of Lendenmann is needed here - it expressly discloses the features required by the claims via its description of the DCE system--including "requesting a network address associated with the secure name" and "receiving a message containing the network address associated with the secure name. Request at 111-114. Moreover, that these features may be optionally implemented within the DCE system does not mean Lendenmann does not disclose a system that comprises those features."

The Examiner agrees with the third party requestor that for reasons previously provided. With regard to the "picking and choosing" argument, these are all features available in Lendenmann, and if a combination of the features described in Lendenmann are usable together, then it properly rejects the claims.

e.

Patent Owner argues that Lendenmann "To the extent Requester implies that use of X.500 names is inherent in these RPC features, it is not necessarily the case that Lendenmann's system would utilize X.500 names during security-enhanced communications. In re Robertson, 169 F.3d 743, 745 (Fed. Cir. 1999) (for inherency, the missing descriptive matter must be "necessarily present in the thing described in the reference, and.., would be so recognized by persons of ordinary skill") (emphasis added). Instead, Lendenmann's DNS and X.500 names are security-independent and are provided merely as alternative DCE-compatible naming schemes "[f]or interoperability purposes." (Lendenmann 21, 71, 192; Keromytis Decl. ¶ 70.) Lendenmann's security features are left in the complete discretion of its user-clients, as discussed above. (Id.)”

The Third party requester responds that “Patent Owners employs a fundamentally implausible reading of Lendenmann - that it "its RPC- related security features ... [do not] .... have anything to do with the allegedly secure (X.500) .... names?' In other words, Patent Owner contends that the secure names in Lendenmann have nothing to do with the mechanisms that ensure secure communications to destinations associated with those names. Obviously, Patent Owner is incorrect. Moreover, Patent Owner again attempts to read non-existent limitations into the claims. In reality, Lendenmann discloses exactly what the claims require: "sending a message to the network address associated with the secure name of the second device using a secure commination link." Request at 114-115. The Examiner's rejection of this claim was based on a correct reading of Lendenmann and the claims, and should be maintained.”

The Examiner agrees with the third party requestor Lendenmann further specifically teaches that “When a client establishes authenticated RPC, it can specify the level of protection to be applied to its communication with the server. The protection level determines the degree to which client/server messages are actually encrypted.” Lendenmann at 192.

4. Dependent claims 3-9, 12-15, and 18-23

Patent Owner provides no distinct response

5. Dependent claims 5 and 6

Patent Owner argues that “The Office and Requester assert that Lendenmann discloses these features because it allegedly describes querying the CDS for binding information via encrypted communications and subsequently decrypting the CDS's response. (OA at 7; Req. at 117-21.) In support of these assertions, Requester cobbles together short excerpts gathered from throughout Lendenmann without regard to whether they reflect the actual role that Lendenmann describes for the CDS in establishing RPCs. (Req. at 117-21, citing Lendenmann 21, 34, 57, 182, 186, 192). These assertions are incorrect and fail to support the rejection of claims 5 and 6.”

The Third party requester responds that “Patent Owner is incorrect, as it simply ignores the disclosures in Lendenmann that expressly describe the CDS's implementation into the "security service" of the DCE and the use of RPC routines in order to query the CDS. Request at 117-119. Further, as already demonstrated above, clients can establish a level of protection with an established RPC that "determines the degree to which clienVserver messages are actually encrypted." Request at 119. Accordingly, the Examiner's rejection of claims 5 and 6 was proof.”

The Examiner agrees with the third party requestor as the security service in Lendenmann has been clearly described as providing encrypted communication between devices.

Dependent claim 21

Patent Owner argues that “Lendenmann does not disclose that its CDS may provide both a network address corresponding to an X.500 name (an allegedly secure name) and a DNS name itself (an alleged unsecured name) to the claimed "first device." Nor does Requester assert that it does. (See Req. at 127.) Rather, Lendenmann explains that X.500 and DNS names are used in the alternative to each other, not that they are both used simultaneously. (Lendenmann 24; Keromytis Decl. ¶ 73.)”

The Third party requester responds that “Lendenmann discloses both a secure name and unsecured name for a given cell. As explained in the Request, DCE makes use of both X.500 naming scheme and DNS, a global addressing and routing scheme that describes unsecured names. Request at 127, The Request also explains that the DCE system includes a function called "cell-name aliasing" which permits devices to have "a primary name, and one or more alias names that is recognized by DCE services in addition to the primary name," such as a primary X.500 name and DNS name as the cell alias. Request at 111-12.”

The Examiner agrees with the third party requestor, just because a device has a secure name does not alleviate the fact that it still has an internet address associated with it.

7. Independent Claim 24 and Dependent Claim 25

Patent Owner argues that The Office and Requester, having earlier asserted with respect to claims 1 and 2 that X.500 names are "secure" while DNS names are "unsecured," now change their position by asserting that all names stored within the CDS are "secure," whether X.500 or DNS. (OA at 7; Req. at 134.) As its basis for this drastic expansion in its position, Requester explains that the Security Service must authenticate and authorize a user before the CDS completes any name-service operations. (Req. at 134, citing Lendenmann 23.) But Requester's assertion that all names within the CDS namespace are "secure" is contrary to the clear teachings of Lendenmann, which expressly teaches that implementation of any security features during RPCs lies within the complete discretion of the user-client. (Lendenmann 71, "RPC clients may choose a security level they want to use. Of course, the level they choose must match a level supported by the server," emphasis added; Keromytis Decl. ¶ 74.)

The Third party requester responds that “neither the Office nor the Requester contended that Lendenmann shows that "all names stored in a CDS are secure." Patent Owner's assertions are also entirely irrelevant m the claims, which make no mention of use of "unsecured" names. Apart from these incorrect and irrelevant assertions, Patent Owner presents no response substantively different from its response to claims 1 and 2. Because the rejections of those claims were proper, the rejection of claims 24 and 25 is also proper and should be maintained.”

The Examiner agrees with the third party requestor, all names in the network communication of Lendenmann are somewhat secure, as provided by the “security service" (see pages 9-10), however, DNS carry a direct tie to internet addressing, while X.500 names remain completely independent (see page 23).

8. Independent Claim 26 and Dependent Claim 27

Patent Owner argues that “Claim 26 also recites "requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device," (emphasis added). Requester cites a portion of Lendenmann that generically describes "registering servers in the namespace," but neither this passage nor any other in Lendenmann discloses that a server may be registered with an additional "unique network address" corresponding to another name, much less a "secure" name. (Req. at 142, citing Lendenmann 203.) Requester additionally fails to explain how Lendenmann inherently discloses any such feature, as nothing in Lendenmann requires that allegedly "secure" X.500 names must necessarily correspond to unique network addresses. (See Keromytis Decl. ¶ 75); In re Robertson, 169 F.3d at 745. For example, X.500 and DNS names for the same server might correspond to the exact same network address. (See Keromytis Decl. ¶ 75.)”

The Third party requester responds that “As explained in the Request, the DCE system permits devices anywhere in the DCE system to obtain the network address of any, other advice to engage in communications. Request at 141. The X.500 naming convention requires each device to be discoverable using both its unsecured name (e.g., the domain name) and its secure name (e.g., the X.500 secure identifier). The X.500 and domain names associated with a device in the Lendenmann scheme thus comprise both a unsecure and a unique secrete network address.”

The Examiner agrees with the third party requestor, the whole purpose of addressing is for the locating of unique network locations, where Lendenmann teaches means for providing naming to network ends where the name corresponds to a specific network address.

9. Independent Claim 28

Patent Owner provides no distinct response

9. Independent Claim 29

Patent Owner provides no distinct response

G. Lendenmann in View of Beser (ISSUE 7)

Patent Owner only argues for "reasons discussed above".

H. Lendenmann in View of RFC2401 (ISSUE 8)

Patent Owner only argues for "reasons discussed above".

I. Provino (ISSUE 9)

1. Overview

Provino teaches use of an unsecured name where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43). Provino further teaches use of a secure name where the device my only establish a secure communication link upon receipt of the secure name (the integer Internet address which is registered on the VPN name server (see column 9, line 56 through column 10, line 7, column 9, lines 17-27, and column 13, liens 26-67), Provino teaches that "*the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30.*" (see column 13, lines 54-67) Here the initiating device has the email address / domain name and requests the actual IP address.

2.

a. "a first device associated with a secure name and an unsecured name"

Patent Owner argues that "Requester has not identified any device in Provino that is associated with both a "secure name" and an "unsecured name.""

The Third party requester responds that "Provino discloses two name servers, Name Server I7 and VPN Name Server 32. Request at 168. Provino also discloses two names are associated with servers on Virtual Private Network 15. The first, a secure name, is the domain name associated with a given VPN server (item 3 I(S), for example), stored in the VPN Name Server 32. The second, an unsecure name, is the domain name of firewall 30, which is also associated with each of the VPN servers (item

3 l(s), for example,). Request at 168; see also Fig. 1. Thus, Provino plainly does show a first device associated with a secure name and unsecure name. Patent Owner's contention that the Request "has not identified any device in Provino that is associated with both a "secure name" and an "unsecured name" is, thus, both wrong and improperly reads non-existent limitations into the term "associated.""

The Examiner agrees with the third party requestor that Provino teaches use of an unsecured name where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43). Provino further teaches use of a secure name where the device my only establish a secure communication link upon receipt of the secure name (the integer Internet address which is registered on the VPN name server (see column 9, line 56 through column 10, line 7, column 9, lines 17-27, and column 13, liens 26-67). The VPN server is associated with the firewall that provides access to it.

b. “secure name”

Patent Owner argues that “Provino, however, does not disclose any "secure names." As disclosed and claimed in the '181 patent, "secure names" are those names used to communicate securely that are resolved by a secure name service (i.e., a service that both resolves a name into a network address and further supports establishing a secure communication link). (Keromytis Decl. ¶ 80.) The name servers in Provino, on the other hand, are conventional name servers of the type distinguished in the '181 patent specification and do not qualify as a "secure name service" that can resolve "secure names." (Id.) The ' 181 patent discloses that a conventional domain name service system merely returns an IP address corresponding to a domain name. (Id. ¶ 81.) For example, in one embodiment, the '181 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name 'Yahoo.corn,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser .... " ('181 patent 38:54-59; Keromytis Decl. ¶ 81; see also '181 patent 38:61-39:13.)

The Third party requester responds that “Owner's analysis is both irrelevant and incorrect. First, the only "secure name service" identified in the Request is VPN Name Server 32; Patent Owner's analysis of Name Server 17 here is irrelevant. Request at l68. Second, the role of VPN Name Server 32, as explained in the Request, is no different than the definition Patent Owner provides in its response: "a service that both resolves a name into a network address and further supports establishing a secure communication link." Response at 45. Indeed, the Request explains that VPN Name Server 32 "serves to resolve human-readable Internet addresses for servers 31 (s) internal to the virtual private network 15 to respective integer Internet addresses, Request at 168. Further, VPN Name Server 32 is not accessible in the same manner as a conventional domain name service. As described in the Request, the secure communication link with the second device is facilitated by VPN Name Server 32, which only provides an authorized device with the second device's secure name. Request at 169.”

The Examiner agrees with the third party requestor, communication in Provino that are authenticated are provided over a secure tunnel, where the firewall provides the device with the identification of the name server, so that the device can access to obtain the appropriate integer Internet addresses for the human readable Internet addresses which may be provided by the operator.

c. “first device”

Patent Owner argues that “Because the claims require that the "first device" be "associated with a secure name and an unsecured name," Provino does not disclose the claimed "first device" for the reasons discussed above in Sections (I)(2)(a) and (b). Accordingly, Provino does not disclose the following features, which also require the undisclosed "first device": * receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device; and * sending a message over a secure communication link from the first device to the second device.'”

The Third party requester responds that “Claim 1 specifies simply "receiving, at a network address corresponding to the secure name associated with the first device, a message, from a second device of the desire to securely, communicate with the first device." Provino unquestionably shows this - the Request explains that Provino shows device 12(m), identified repeatedly above as the claimed "second device," sends "a message packet for transfer from the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30." Request at 171. Rather than respond substantively to this, Patent Owner asserts the Request "mixes and matches features from different devices in its attempt to show unpatentability" Response at 45-46. Patent Owner's assertion is irrelevant, as it simply ignores the actual disclosure of Provino,"

The Examiner agrees with the third party requestor, device 12(m) which is one of multiple networked devices, sends a message requesting establishment of a secure channel and then communicates via the secure tunnel.

d. "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device"

Patent Owner provides no distinct response

3. Independent Claim 2

Patent Owner only argues for "reasons discussed above".

4. Dependent Claims 3-15 and 19-22

Patent Owner only argues for "reasons discussed above".

5. Dependent Claim 23

Patent Owner only argues for “reasons discussed above”.

6. Dependent Claim 28

Patent Owner only argues for “reasons discussed above”.

7. Dependent Claim 29

Patent Owner only argues for “reasons discussed above”.

J. Provino and H.323 (ISSUE 10)

1. Independent Claim 24 and Dependent Claim 25

Patent Owner only argues for reasons discussed above and “reasons discussed in more detail below”.

2. Independent Claim 26

Patent Owner argues that “H.235, however, is not incorporated by reference into H.323 and is therefore not properly considered to be part of that document. Section III.K. 1 below provides additional details on why it is legally and factually improper to include it in the rejection as though it were incorporated by reference into H.323. For now, it is sufficient to note that the Requester's proposed rejection is both legally and procedurally deficient and can be withdrawn on that basis alone.”

The Third party requester responds that “As explained in the request, H.323 expressly incorporates H. 235 as "constituting provisions of this [i.e., the 1t.323] Recommendation." Request at 204 (citing H.323 at 2-3). Accordingly, Patent Owner's "procedural" argument is wrong. Further, Patent Owner's so-called "substantive []" arguments with respect to these claims present no distinct response from that offered in claim 1. Because the rejection of claim 1 was proper, the rejection of claim 26 based on Provino in view of H. 323 was also proper and should be maintained.”

The Examiner agrees with the third party requestor, H235 is being referenced as a standard for security and encryption of H-Series multimedia terminals, specifically noting H.323.

K. H.323 (ISSUE 11)

1.

Patent Owner argues that “The Office and Requester contend that H.323 expressly incorporates the reference "H.225.0 Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems" ("H.225"), the reference "H.235 Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals" ("H.235"), and the reference "H.245 Control Protocol for Multimedia Communication" ("H.245"). (Req. at 204.) The Request states that H.225, H.235, and H.245, are "incorporated by reference because they are specifically referenced and described as disclosing particular features of the H.323 recommendation." (Id.) This is incorrect.

To incorporate matter by reference, a host document must contain language "clearly identifying the subject matter which is incorporated and where it is to be found." In re de Seversky, 474 F.2d 671,674 (CCPA 1973). A "mere reference to another application, or patent, or publication is not an incorporation of anything therein." Id. Put differently, "the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents." Adv. Display Sys., Inc., 212 F.3d at 1282 (emphasis added).

H.323 does not identify with detailed particularity the subject matter of H.225, H.235, and H.245 allegedly incorporated."

The Third party requester responds that "The Examiner correctly found that the above-cited H-series recommendations are expressly incorporated as part of the disclosure of H.323, which anticipates claim 1. In response, Patent Owner asserts that if 323 does not properly incorporate the teachings of H. 323, H.245, H.235, and H.225 because H.323 "does not identify with detailed particularity the subject matter' of those references. Response at 52. Patent Owner is incorrect. First, as explained in the request, H.323 expressly incorporates H.245, H. 231 and H.245 as "constituting provisions of this [i.e., the H.323] Recommendation." Request at 204 (citing H. 323 at 2-3), That is sufficient. See Harari v. Lee, 656 F.3d 1331, 1335 (Fed. Cir. 2011)(holding "broad and unequivocal" language sufficient to incorporate the entire disclosure of another reference), Even under the previous standard cited by Patent Owner, each of H. 245, H.235, and H.245 was properly incorporated by reference into H.323, For example, H.323 explains that "authentication and security for H.323 is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235, H.323 at 81 (emphasis added). Similarly, H.323 discloses that products claiming compliance with Version 2 of H.323 shall comply with all of the mandatory requirements of H.323 (1998)which references Recommendations H.225 (1998) and H.245 (1998)," H. 323 at (i) (emphasis added). H1323 also describes H.225 as containing "[c]all signaling protocols and media stream packetization for packet based multimedia communication systems," and H.245 as containing "[c]ontrol protocol for multimedia communication," H.323 at 2-3, H.323 thus clearly incorporates by reference the teachings of H.225, H.235, and H.245. Accordingly, the Examiner's rejection of this claim was proper mad should be maintained."

The Examiner agrees with the third party requestor as H.323 specifically states:

> *"The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendations"*

This statement is then followed by the Recommendations for H.225, H.235, and H.245, amongst others.

2. Overview of H.323

3.

a. “a First Device Associated with a Secure Name and an Unsecured Name”

Patent Owner argues that “Independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." The combined H. 323 references do not disclose these claim features.”…“The Office and Requester's allegation that the URL for a gatekeeper corresponds to the unsecured name recited in independent claim 1 is incorrect. (Keromytis Decl. ¶ 92.)”…“The Office and Requester also allege that if the H.323 endpoint is a Gateway, (see Req. at 211), a first SCN endpoint that is obtaining access to the PBN through the Gateway has an unsecure name. (Req. at 212-13.) This is also incorrect. (Keromytis Decl. ¶ 93.)”

The Third party requester responds that “As explained in the Request, ft. 323 discloses that each device in an H.323 network "is associated with one or more alias names, called Alias addresses, which can be in the form of a phone number or an email address." Request at 204. Alias addresses are "secure," in part, because they are "protected by 'access tokens,' which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses." Request at 204. Further, the Requester notes again that during prosecution of the '181 patent, for example, the Patent Oyster explained that a "secure name" is registered in a "secure name registry" mad can include a "secure domain name," but can be as basic as a "telephone number." Order at 5. And, in a related patent reexamination, the Patent Owner explained that "a conventional domain name service cannot resolve a secure domain name." Id Thus, under the broadest reasonable construction, a "secure name" is defined both by storage in a "secure name registry," and because it cannot be resolved by a conventional domain name service. According to Patent Owner, a telephone number, such as the "alias address" described in H.323, would satisfy this construction."

…"secure names, the Request explains, are registered with a "Gatekeeper" in addition to "be[ing] associated with the unsecured names of the Gatekeeper computer with which they are registered." Request at 210, In response, Patent Owner contends that the Request has not identified any device in H. 323 that is associated with both a "secure name" and an "unsecured name." Response at 45, Patent Owner's response attempts to read non-existent limitations into the term "associated"-the plain language of this term refutes Patent Owner's assertions."

The Examiner agrees with the third party requestor that a generic name associated with a network location such as a phone number or email address can correspond to the Patent Owner's described secure name, as the name and address are linked via a registry. Where the address itself (capable of accessing the network end), is an unsecure means of access.

b. "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire to Securely Communicate with the First Device

Patent Owner argues that "H.323 does not describe receiving any message at a network address corresponding to an access-token-protected alias rather than a second, allegedly "unsecured" alias. Nor does the Request assert that it does. (See Req. at 213-14.) Furthermore, H.323 discloses that its access tokens merely "shield[] an endpoint's Transport Address and Alias Address," and therefore H.323 does not disclose any "message ... of the desired to securely communicate." (H.323 38; Keromytis Decl. ¶ 98.) As explained above with respect to Beser, merely shielding the endpoints of communications does "not secure those communications from eavesdropping." (Supra Section III.B.2.c.ii.) And therefore, any access-token-related messages do not communicate a "desire[] to securely communicate," as recited in claim 1. Thus, the rejection is improper and should be withdrawn."

The Third party requester responds that "Patent Owner ignores the Request and the H. 323 disclosure, which clearly explain that one endpoint receives a request from another endpoint of the desire to communicate securely, and that these endpoint may further be protected by "access tokens," which are utilized to "obscure or hide destination addressing information." Request at 213-17. As for Patent Owner's statement that "as explained above with respect to Beser, merely shielding the endpoints of communications does 'not secure those communications from eavesdropping'"--the Examiner has already found that statement to be irrelevant, as described above. See also ACP at 32-22 ("Encryption is more secure than hiding the source address just as encryption and hiding the address is more: secure than encryption only. The claims however do not recite the degree of security.")"

The Examiner agrees with the third party requestor that H. 323 provides a request to communicate using the secure naming structure described above.

Patent Owner argues that “regardless of whether H.235 is incorporated into H.323, it nevertheless fails to disclose receiving any "message . . . of the desire[] to securely communicate" at a network address corresponding to any access-token-protected alias address (i.e., alleged secure name). Without identifying any message in particular, the Requester points to at least five sections of H.235 as disclosing these features. But despite citing these different passages, Requester fails to point out any single message in support of its arguments. The rejection should be withdrawn for this reason.”

The Third party requester responds that “Response at 57. Patent Owner is mistaken. As explained in the Request, the second device, i.e., '~the calling endpoint," together with its "gatekeeper," would establish a "call signaling channel" by retrieving and communicating the "address and port number of the call signaling channel in the called endpoint." Request at 215. After establishing the "call signaling channel" (which is used to carry call control messages), the "endpoints can negotiate the use of IPSEC for the H.245 channel" on the “Q.931 SETUP and CONNECT exchange." Request at 216. During the Q.931 SETUP and CONNECT exchange process, the Gatekeepers will facilitate, for example, "routed call signaling." H.323 at Fig.23 at 51-52 ("Endpoint I (calling endpoint) initiates the ARQ (1)/ACF (2) exchange with Gatekeeper 1. Gatekeeper 1 shall return a Call Signaling Channel Transport Address of itself in the ACF (2). Endpoint 1 then sends the Setup (3) message using that Transport Address. Gatekeeper 1 then sends the Setup (4) message to the well-known Call Signaling

Channel Transport Address of Endpoint 2. If Endpoint 2 wishes to accept the call, it initiates the ARQ (6)/ACF (7) exchange with Gatekeeper 2.2?'). Patent Owner's argument that the communication in 1-1. 323 "occurs only after security features have been employed" is also incorrect; The Request explains that the endpoints negotiate the use of IPSEC during the setup process, Request at 216. Patent Owner next contends that the "call control (H.245) security" and "media stream privacy" do not support the rejection because "these passages do not describe receiving any message at a network address corresponding to an access token or an access-token protected alias address." Response at 58. Patent Owner is incorrect for the reasons stated above. Further, Patent Owner seems to contend that it is significant that certain security features may' be within the discretion of the calling endpoint. Response at 58. Patent Owner's assertion is irrelevant, as the fact that the calling endpoint may choose to implement IPSEC is exactly what the anticipated claim calls for, i.e., "a message from a second device of the desire to securely communicate with the first device." Accordingly, the Examiner was correct to find that 11. 323 discloses this limitation."

The Examiner agrees with the third party requestor, as a request for the session initiation is provided followed then either by an accepted or rejected decision by the other network end, where the gatekeeper acts and an intermediary to control access.

c. "Sending a Message over a Secure Communication Link from the First Device to the Second Device"

Patent Owner “raises no new arguments” in response to the above claim limitation.

4. Independent Claim 2

a. “a Secure Name”

Patent Owner only argues that the reference is lacking "for at least similar reasons as discussed above".

b. “a Network Address Associated with the Secure Name of the Second Device”

Patent Owner argues that “The Office and Requester fail to identify with any specificity what teaching in the combined H. 323 references corresponds to the "network address associated with the secure name of the second device," as recited in claim 2.”

The Third party requester responds that “As explained in the Request and above, after establishing the "call signaling channel" (which is used to carry call control messages), the "endpoints can negotiate the use of IPSEC for the H.245 channel" on the “Q.931 SETUP and CONNECT exchange," Request at 216, In turn, during the Q.931 SETUP and CONNECT exchange process, for example, the Gatekeepers will facilitate "routed call signaling." H.323 at Fig.23 at 51-52 (endpoint 1 (calling endpoint) initiates the ARQ (1)/ACF (2) exchange with Gatekeeper 1. Gatekeeper 1 shall return a Call Signaling Channel Transport Address of itself in the ACF (2). Endpoint l then sends the Setup (3) message using that Transport Address. Gatekeeper 1 then sends the Setup (4) message to the well-known Call Signaling Channel Transport Address of Endpoint 2. If Endpoint 2 wishes to accept the call, it initiates the ARQ (6)/ACF (7) exchange with Gatekeeper 2.2."), Accordingly, the Examiner's finding that H.323 discloses this element was correct."

The Examiner agrees with the third party requestor, as a request for the session initiation is provided followed then either by an accepted or rejected decision by the other network end, where the gatekeeper acts and an intermediary to control access.

c. "from the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated with the Secure Name of the Second Device" and "at the First Device, Receiving a Message Containing the Network Address Associated with the Secure Name of the Second Device"

Patent Owner argues that "the Office and Requester fail to identify with any specificity what teaching in the combined H.323 references corresponds to the "message requesting a network address" or the "message containing the network address" recited in claim 2"

The Third party requester responds that "even assuming that the "alias addresses" required the "access token" feature to be considered "secure names," H.323 satisfies the above claim requirement nonetheless. As explained in the Request, "calls using the Access Token can be routed through the Gatekeeper to the called endpoint?' Request at 220. In such situations, the Access Token identifies the Gatekeeper, and particularly the address of the Gatekeeper in order to communicate with a given endpoint. Patent Owner next contends that "a calling endpoint using an access token never receives a network address associated with the access-token-protected alias address." Response at 60. Yet, the claims impose no such requirement, and Patent Owner's response which presumes this to be the case should be disregarded, as it attempts to read non-existent limitations into the term "associated."

The Examiner agrees with the third party requestor that by returning the address of the gateway associated with the second device is sufficient to read on the claim. See H.235 at 28.

Patent Owner argues that “because a calling endpoint using an access token never receives a network address associated with the access-token-protected alias address, H.323 does not disclose "receiving a message containing the network address associated with the secure name of the second device," as recited in claim 2. (Keromytis Decl. ¶ 108.) Requester additionally relies on the security token passage of H.235 as disclosing the "sending a message to a secure name service" and "receiving a message containing the network address" features of claim 2. (Req. at 218-23.) But even if one incorrectly assumed that H.235 could be incorporated by reference into H.323, the H.235 security token feature does not utilize an alias address protected by an access token. (H.235 28-29; Keromytis Decl. ¶ 109.) Accordingly, it does not disclose "sending a message.., requesting a network address associated with the secure name of the second device," and "receiving a message containing the network address associated with the secure name." Indeed, the Office and Requester cannot point to the use of security tokens in H.235 as providing an example of using access tokens. Nowhere does H.323 or H.235 disclose that an access token is the same as a security token."

The Third party requester responds that "Patent Owner is incorrect. First, the disclosed "access tokens" are an additional feature of the H. 323 system that contribute an additional element of security to the disclosed point-to-point communications. Request at 219-21. So, while an "access token,' may be sufficient to render an "alias address" a secure name, "access tokens" are not necessary, Patent Owner's remaining arguments with respect to this limitation hinge on this incorrect assumption. Response at 60-62. As explained above, Patent Owner has represented that a "secure name" can, like the "alias addresses" of H. 323, be as basic as a telephone number""

The Examiner agrees with the third party requestor that again these are levels of security, where each of the references desire for layers of securing information show a layering of hidden addresses, encryption, and other means of securing network communications.

d. "From the First Device, Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

Patent Owner “presents no arguments that are distinct from those already presented with respect to other requirements of claims 1 and 2".

e. Dependent Claims 3, 6-7, 12, 14-20, 22, and 23

Patent Owner presents “no distinct response”.

f. Dependent Claim 4

Patent Owner argues that “Requester bases its "secure name" arguments regarding the H. 323 access token section and the H.235 IPsec passages on extraneous features that merely shield names from other entities. Thus, the combined H.323 references do not disclose that the names themselves indicate any security. (Keromytis Decl. ¶ 114.)”

The Third party requester responds that “the Request demonstrates that these endpoints may further be protected by "access tokens," which are utilized to "obscure or hide destination addressing information." Request at 220. The access tokens, which obfuscate the destination address information, thus "indicate security." See also ACP at 32- 32 ("Encryption is more secure than hiding the source address just as encryption and hiding the address is more secure than encryption only. The claims however do not recite the degree of security.") Consequently, the Examiner's rejection of claim 4 was proper.”

The Examiner agrees with the third party requestor that the reference uses layered security measures to meet a certain level of security that all security measures combined provide.

g. Dependent Claim 5

Patent Owner presents “no response distinct from its response to the rejection of claim 2”.

h. Dependent Claim 9

Patent Owner argues that “Without providing any shred of support, Requester makes the conclusory assertion that any alleged communication link would be initiated automatically. Mere attorney argument fails to support the § 102(b) rejection, as anticipation requires that "each and every element as set forth in the claim [be] found, either expressly or inherently described, in a single prior art reference." Verdegaal 814 F.2d at 631. The rejection should be withdrawn.”

The Third party requester responds that “H.323 describes processes that would be both automatic and transparent to the user, For example, H.323 explains that "[a]fler obtaining the address and port number of the call signaling channel, the: calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair," Request at 219. These steps occur without any interaction from the endpoint that originally made the request to engage in secure communications,"

The Examiner agrees with the third party requestor that the steps are automated via the computer system without further user interaction.

i. Dependent Claims 10 and 11

Patent Owner argues that "The Office asserts that the tunneling features of claims l0 and 11 are disclosed by the "Encapsulation" passage ofH.323. (OA at 11-12, quoting H.323 59.) But this passage does not disclose receiving any message containing a network address "through tunneling," as recited in claim 10, or "in the form of at least one tunneled packet," as recited in claim 11. (Keromytis Decl. ¶ 116.) This is unsurprising, because the tunneling discussed on page 59 involves H.245 channels and messages, while the gatekeeper (alleged to correspond to the "secure name service") communicates with endpoints through H.225 signalling. (H.323 27.) The Office and Requester do not identify any additional passage disclosing these combined features, as the H.235 IPsec passage cited in the Request only discloses an address corresponding to a "call signalling channel"--not an endpoint (i.e., alleged "second device")--as discussed above. (See OA at 11-12; Req. at 231.)"

The Third party requester responds that with respect to "Patent Owner contend(ing) that the "Request only discloses an address corresponding to a 'call signaling channel'--not an endpoint (i.e., alleged "second device")." Patent Owner is incorrect for the reasons explained above." "Further, the Office Action explains that "when tunneling is active, one or more H. 245 messages can be encapsulated in any Q. 931 message..," OA at 12, Encapsulating a Q.931 message, of course, would include "Q.931 SETUP" messages, which involve the negotiation and establishment of the secure communication link. Accordingly, the Examiner's rejection of these claims was proper and should be maintained, See also Request at 230-231."

The Examiner agrees with the third party requestor that H.245 messages are capable of being encapsulated in a Q.931 message.

j. Dependent Claim 13

Patent Owner argues that "Requester's argument is belied by the very passage it cites. H.323 explains that its layering feature should employ a separate channel and a separate session, unlike the additional feature of claim 13, which recites that one "secure communication link includes multiple sessions." (H.323 at 91; Keromytis Decl. ¶ 117.) Moreover, as discussed above with respect to claims 1 and 2, the combined H. 323 references do not disclose any "secure communication link," as recited in claim 13. The rejection should be withdrawn."

The Third party requester responds that "The Examiner correctly found that H.323 discloses every limitation of claim 13, which specifies that the "receiving and sending of messages through the secure communication link includes multiple sessions." As explained in the Request, H.323 employs "multiple logical channels and RTP sessions" over a secure communication link. Request at 232-233. In response, Patent Owner contends that H. 323 does not disclose this requirement because the H.323 layering technique "should employ a separate channel and separate session." Response at 64. As Patent Owner's comment acknowledges, this manner of implementation is option to the H.323 processes, Response at 65, Patent Owner's response also reads non-existent limitations into the term "secure communication link," As the claims are not so limited, the rejection as imposed was proper and should be maintained."

The Examiner agrees with the third party requestor, H.323. provides specifically for the use of multiple sessions (see pages 91 and 73).

k. Dependent Claim 21

Patent Owner presents no response that is distinct from those answered above.

l. Independent Claim 24 and Dependent Claim 25

Patent Owner presents no response that is distinct from those answered above.

m. Independent Claim 26 and Dependent Claim 27

Patent Owner presents no response that is distinct from those answered above.

n. Independent Claim 28

Patent Owner presents no response that is distinct from those answered above.

o. Independent Claim 29

Patent Owner presents no response that is distinct from those answered above.

L. Johnson in view of RFC 2131, RFC 1034, and RFC 2401 (ISSUE 13)

1. Overview of Johnson

Johnson teaches a secure name being registered by the secure mail server with the secure name server. (see column 10, lines 36-52). Johnson discloses that the a first device securely communicated with the secure name server in order to request a network address that is associated with the secure name--which is associated with the network address---of the second device, i.e., the secure mail server. At 11:21-37, Johnson explains: *Process to Get an Address from a Secure Name Server FIG. 7 of the drawings outlines the process by which an unknown address, such as* ***the dynamic address of a secure mail server, is obtained from a secure name server.*** *The process starts by selecting the target secure name server machine by its fixed address/name as shown in block 150. The user then provides the secure name server with its logon protocol combination as shown at block 152. If the user logon combination is verified then a session is established with a secure name server as shown at block 154. ...if the session has been correctly established as shown at block 156, then the user will be allowed to request the address for the named machine at the client site as shown at block 158.*

2. Overview of RFC 2131, RFC 1034, and RFC 2401

RFC 2131, RFC 1034, and RFC 2401 specify how a Dynamic Host Configuration Protocol server provides a framework for passing configuration information to hosts on a TCPIP network.

3. Independent Claim 1

a. "A First Device Associated with a Secure Name and an Unsecured Name"

Patent Owner argues that "The secure name server 14 in Johnson, on the other hand, is a conventional name server of the type distinguished in the '181 patent specification and does not qualify as a "secure name service" that can resolve "secure names." (Keromytis Decl. ¶ 121.) Instead, when provided with the name of secure mail server 16, the secure name server 14 merely returns the dynamic address of the secure mail server 16. (Id.) Johnson does not disclose that secure name server 14 provides any further support for establishing a secure communication link. (Id.)"

The Third party requester responds that "Patent Owner made representations during prosecution of the related '180 patent about the meaning of the terms "secure name" and "secure name service" that were different than its present assertions. Office Action at 5. Specifically, Patent Owner stated that a" "secure name' is a name associated with a network address associated of a [SIC] first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device." Order at 5 (emphasis added). The Secure Name Server 14 disclosed in Johnson at least satisfies this broad construction. Patent Owner's claim that Secure Name Server 14 "is a conventional name server" is also simply incorrect. As described in the Request, the secure communication 1~ with the second device is facilitated by Secure Name Server 14, which only provides a network address associated with a secure name to an authorized requesting device. Request at 272-75. A conventional name server would not have such security features in place. Finally, Patent Owner's argument that secure name server 14 does not provide "any further support for establishing a secure communication link" is baseless. Indeed, nothing in the claim or in Patent Owner's representations to the Patent Office requires that a secure name service '~provide any further support for establishing a secure communication link." Patent Owner again attempts to improperly read non-existent limitations into claim 1."

The Examiner agrees with the third party requestor, the security features utilized by the Secure Name Server 14 make it distinct from a conventional name server, by requiring protected access.

Patent Owner argues that "Johnson does not meet it, because Johnson does not teach or suggest that the name of secure mail server 16 is protected through authorization and encryption. (Keromytis Decl. ¶ 122.) Instead, the user accessing the secure name server 14 must presumably already know the name of the secure mail server 16 before the alleged authorization and encryption ever happens, because if the user did not already know the name, it would not know how to request any information regarding the secure mail server 16 from secure name server 14. (Id.) There is no disclosure in Johnson regarding how the user initially learns this name, whether authorization is required before obtaining the name, or whether encryption is used in providing the name. (Id.)”

The Third party requester responds that “Patent Owner's analysis is incorrect and irrelevant. First, as demonstrated above, the Request shows that Johnson discloses a "secure name" under Patent Owner's own interpretation of that term. Second, Patent Owner next contention- "the user accessing the secure name server 14 must presumably already know the name of the secure mail server before the alleged authorization and encryption" - again tries to read non-existent limitations into the claims. Response at 68. Nothing in specification or claims requires that a secure name not be "known" in advance of a request to access that name.”

The Examiner agrees with the third party requestor, the user at the first device requests access to the secure mail server via a "name” (secure) then when they are authenticated via the secure name server, they are provided with the “address” (unsecure) corresponding the provided “name" (see 11:20-37).

Patent Owner argues that “Requester never argues that secure name server 14 is the claimed "first device associated with a secure name and an unsecured name." Instead, Requester alleges that secure mail server 16 is the claimed "first device." Thus, it is irrelevant whether secure name server 14 has an unsecured name, as it has no bearing on the claims. The second reason is that both allegations (regarding registration of secure name server 14 with a DHCP server or in the public DNS system) appear to rely on the premise that the secure name server 14 must have a registered domain name, which the Office and Requester allege is "necessary to the invention of Johnson" for Johnson to be used in "communications over the Internet." (Req. at 274.) This premise is incorrect because a registered domain name is not a prerequisite for communications over the Internet. (Keromytis Deck ¶ 124.) "... "Office and Requester allege that "the secure mail server has a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an 'unsecured name'." (Req. at 274.) Requester cites no support for this statement (see id.), and the statement is incorrect because the secure mail server 16 is only disclosed to have its name registered in secure name server 14. (Keromytis Decl. ¶ 125.)"

The Third party requester responds that "The Request also explained that where the secure server name is used to conduct transactions over the Interact, that would be done consistent with established Internet standards (e.g., RFC 1034). See Request at 273-274. The Request explained in that embodiment, it would be known to use a registered domain name, as that was commonplace at the time. Id. Patent Owner's convoluted hypothetical at page 69 of the Response, thus, ignores the actual claim language and severely mischaracterizes the Request. Patent Owner also contests the description of Johnson, asserting that it does not indicate "the secure mail server has a domain name registered in the public DNS system and/or a client identifier associated with such domain that constitutes an 'unsecured name?" The Request at 273-274 reproduced excerpts from Johnson and explained why this description, contrary to Patent Owner's assertions, is correct Moreover, Patent Owner has not explained how this particular detail is relevant to the claim 1. In reality it is not.

The Examiner agrees with the third party requestor, the user at the first device requests access to the secure mail server via a "name" (secure) then when they are authenticated via the secure name server, they are provided with the "address" (unsecure) corresponding the provided "name" (see 11:20-37).

b. "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire[] to Securely Communicate with the First Device"

Patent Owner argues that "The references are also lacking regarding the "message from a second device of the desire[] to securely communicate with the first device." The Office and Requester contend that the claimed "message" is Johnson's email message from first user 12 to second user 18. (Req. at 275; see Johnson 7:10-11.) This communication is provided by the first user 12 to second user 18's mailbox on secure mail server 16. (Johnson 7:20-27.) Since the content of the message is destined for second user 18, Johnson does not disclose that it contains any information intended for use by secure mail server 16 (i.e., the alleged "first device"), let alone any indication of a desire to securely communicate with the secure mail server 16. The Office and

Requester do not allege that the other cited references cure this deficiency of Johnson. (See Req. at 274-75.)"

The Third party requester responds that Patent Owner asserts that Johnson does not describe systems showing this element because Johnson °does not disclose or suggest a 'secure name,'" relying on its arguments above. But, as already demonstrated, Patent Owner is incorrect, Patent Owner also contends that the references "are lacking regarding the 'message from a second device of the desire[] to securely communicate with the first device," Patent Owner's analysis is simply wrong, As explained in the Request, the "first user 12" utilizes the prescribed authentication procedures and the network address of the secure mail server 16 in order to send an "electronic mail message protected by a protection method, such as encryption.., to the designated recipient's box on the secure electronic mail server 16," Request at 275. Accordingly, Johnson describes this element of claim 1,

The Examiner agrees with the third party requestor that Johnson teaches a process that begins with selecting the target secure name server machine by its fixed name as shown in block 150. The user then provides the secure name server with its logon protocol combination as shown at block 152. If the user logon combination is verified then a session is established with a secure name server as shown at block 154.

c. "Sending a Message Over a Secure Communication Link from the Frist Device to the Second Device"

Patent Owner argues that Johnson should be read to suggest only one-way communications.

The Third party requester responds that “This is an obviously implausible - reading of Johnson. Plainly, the so-called "first device" of Johnson may function as a "second device" depending upon which device in Johnson initiates the secure communication. Accordingly, the Examiner's rejection of the claim was proper and should be maintained. See also Request at 270-276.

The Examiner agrees with the third party requestor that bidirectional communication between the mail server and the user is a clear feature of Johnson.

4. Independent Claim 2

Patent Owner provides not distinct response from those submitted and answered above.

5. Dependent Claims 4-6, 8, 12, and 17-20

Patent Owner provides not distinct response from those submitted and answered above.

6. Dependent Claim 3

Patent Owner argues that “the Office and Requester allege that the Domain Name System ("DNS") teachings of RFC 1034, combined with Johnson, disclose or suggest that the name of the secure mail server 16 can be a secure domain name. (Req. at 283-284.) In support of this allegation, the Office and Requester combine RFC

1034's teaching of an authoritative name server with the secure name server 14 of Johnson to conclude that the secure name server 14 is "the authoritative name server for the protected network." (Req. at 283- 284.) The Office and Requester, however, provide no reasoning supporting this conclusory allegation. (See id.) There is no indication of how Johnson would determine which of its multiple name servers, if any, would function as the authoritative name server. (See id. at 282-84; see also Keromytis Decl. ¶ 130.)"

The Third party requester responds that "Patent Owner asserts that Johnson in view of RFC 1034 does not "disclose or suggest that the name of the secure mail server 16 can be a secure domain name?' Response at 71. Patent Owner is incorrect. The Request explains that a person of ordinary skill in the art would have found motivation within Johnson to modify the secure communications disclosed therein to incorporate additional mechanisms to facilitate interbusiness communications by making it possible to locate the secure name server 14 by name, for example, through the public resources of the Internet. Request at 273-74, 82-84. That person would have found in both Johnson and RFC 1034 an identification of the same problem (improving access of interbusiness communications) as well as a solution to the same problem: a user-friendly naming scheme. Consequently, the Examiner's rejection of claim 3 based on Johnson view of RFC 2131, RFC 1034 and RFC 2401 was proper and should be maintained"

The Examiner agrees with the third party requestor, as Johnson already speaks to the benefits of hiding the network address of network ends, rather accessing them through a name and a secure name server that can patch through acceptable communication requests.

7. Dependent Claim 7

Patent Owner argues that “the Office and Requester have not shown that the registration process in any of the embodiments of Johnson utilizes a non-secure communication link. The Office and Requester do not allege that the other cited references cure these deficiencies of Johnson (see Req. at 286-87), so claim 7 is not obvious.”

The Third party requester responds that “Claim 7, in particular, does not impose any restrictions how the secure and non-secure communications may be "supported" by the specified device. As the Request explains, Johnson states that in certain circumstances, it would be appropriate to have the secure name server reside on the same machine as the secure mail server. Request at 287. Johnson explains in that scenario, certain lines of communications would remain encrypted, but does not show that the communications between the secure name server and secure mail server during registration must be secure.”

The Examiner agrees with the third party requestor that the claim is not so limiting to define the level of security, and the claim only state the device be "capable" of secure and non-secure communication, where during registration and local communications security is limited (as it is not necessary).

8. Dependent Claims 9-11 and 13-16

Patent Owner argues that “combining RFC 2401 with Johnson would change the principle of operation of Johnson's system, and therefore there is no motivation to combine Johnson with RFC 2401. In particular, Johnson discloses a system that is allegedly used in "network communications where security is required," (Johnson 1:26.), while RFC 2401 discloses a "[s]ecurity Architecture for the Internet Protocol." (RFC 2401 at 2.) Accordingly, replacing Johnson's system (that is allegedly used in network communications where security is required) with RFC 2401 's security architecture would change the principle of operation of Johnson's system, (i.e., the proposed combination would change the manner in which Johnson's system is used in "network communications where security is required"). Furthermore, the security architecture of RFC 2401, may be redundant to, and may not be interoperable with, the system of Johnson. One of ordinary skill in the art would recognize the folly in this combination and would not have been motivated to make the combination. See In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).”

The Third party requester responds that “is incorrect. As explained in the Request, a person of ordinary skill in the art would have found motivation within Johnson to modify the secure communications disclosed therein to incorporate additional security mechanisms for communications over the Internet, Request at 289-

90. That person would find in Johnson or RFC 2401 identification of the same problem (improving security for Internet Protocol communications) as well as a solution to the same problem: an encryption and/or tunneling scheme. There is nothing in either reference that suggests that one must modify the essential features of the Johnson system to implement IPSec in communications. Because Patent Owner provides no substantive response to claims 9-11 and 13-l6, the Examiner's rejection of those claims based on Johnson view of RFC 2131, RFC 1034 and RFC 2401 was proper and should be maintained."

The Examiner agrees with the third party requestor, the references are both in the same technological area, and solve the same problems, albeit through different network structures.

9. Dependent Claim 21

Patent Owner provides not distinct response from those submitted and answered above.

10. Dependent Claim 22

Patent Owner argues that "The Office and Requester completely fail to address the claimed feature of the secure name being registered "prior to the step of sending a message to a secure name service," as recited in dependent claim 22. (See Req. at 299-300.) Accordingly, the rejection is deficient and should be withdrawn."

The Third party requester responds that “the Request, which clearly explains that the secure email server will “go on to register the dynamic address" of the secure email server 16. See also Request at 299-300. This step, of course, would necessarily take place prior to another device securely communicating with secure email server 16”

The Examiner agrees with the third party requestor, if the secure email server was not previously registered it would not be able to be accessed by name, rendering the secure access of Johnson irrelevant.

11.Independent Claim 24

Patent Owner argues that “Requester has things reversed, as the claim recites "sending a message securely from the first device to the second device," not sending a message from the second device to the first device. Accordingly, the Office and Requester have not shown that Johnson discloses or suggests this feature, and they have not alleged that the other cited references cure this deficiency of Johnson. (See Req. at 301-04.)”

The Third party requester responds that “the only new argument presented by Patent Owner is that the Request "has things reversed, as the claim recites 'sending a message securely from the first device to the second device." Response at 74. Patent Owner is incorrect. As already demonstrated above, certainly Patent Owner would agree that Johnson does not disclose a system that only permits one-way communication and neither does the' 181 patent, for that matter--such that the so-called "first device" of Johnson may be deemed a "second device" within the context of the claim depending upon which device initiates the secure communication. Accordingly, the Examiner's rejection of the claim was proper and should be maintained. See also Request at 301-304."

The Examiner agrees with the third party requestor that the Johnson system is capable of bidirectional secure communication. Johnson further shows supplying received mail messages from the mail server to the user (10:4-26).

12. Dependent Claim 25

Patent Owner argues that "Claim 25 also recites, among other things, "sending a message securely comprises sending the message from the first device to the second device using a secure communication link." The Office and Requester completely fail to address this aspect of claim 25. (See Req. at 304-05.) Thus, the rejection is deficient and should be withdrawn. See Ex Parte Karl Burgess, Appeal 2008-2820, 2009 WL 291172, at *3 (to support an obviousness rejection, "all of the claim limitations must be taught or suggested by the prior art applied and that all words in a claim must be considered .... ")."

The Third party requester responds that "As explained in the Request, "the dynamic address of the secure electronic mail server 16 is not easily obtained" because, for example, it requires "authorization to access and is protected through encryption." Request at 304-05. Thus, Johnson describes "sending a message securely using a secure communication link." Accordingly, the Examiner's rejection of the claim was proper and should be maintained."

The Examiner agrees with the third party requestor that the encrypted channel accessible through a secure name server is a secure transmission line.

13. Independent Claim 26

Patent Owner provides not distinct response from those submitted and answered above.

14. Dependent Claim 27

Patent Owner provides not distinct response from those submitted and answered above.

15. Independent Claim 28

Patent Owner provides not distinct response from those submitted and answered above.

16. Independent Claim 29

Patent Owner provides not distinct response from those submitted and answered above.

M. Secondary Considerations

The Examiner has considered these "secondary considerations" but doesn't see any evidence that precludes use of any of the above maintained prior art rejections.

Conclusion

This is an ACTION CLOSING PROSECUTION (ACP); see MPEP § 2671.02.

(1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.

(2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).

(3) Appeal **cannot** be taken from this action, since it is not a final Office action.

Extensions of time under 37 CFR 1.136(a) will not be permitted in inter partes reexamination proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to the patent owner in a reexamination proceeding. Additionally, 35 U.S.C. 314(c) requires that inter partes reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.937). Patent owner extensions of time in inter partes reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner's response is set by statute. 35 U.S.C. 314(b)(3).

The Patent Owner is reminded of the continuing responsibility under 37 CFR 1.985(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the US Patent 6,564,275 throughout the course of this reexamination proceeding. The Third Party Requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding through the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

All correspondence relating to this ex parte reexamination proceeding should be directed as follows:

By U.S. Postal Service Mail to:

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:

(571) 273-9900
Central Reexamination Unit

By hand to:

Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are “soft scanned” (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the “soft scanning” process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/Dennis G. Bonshock/

Primary Examiner, Art Unit 3992

/JDC/

/Alexander J Kosowski/

Supervisory Patent Examiner, Art Unit 3992

Re - Exam

PATENT
Customer No. 23,630
Attorney Docket No. 077580-0160

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U. S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§ 1.933 AND 1.555

Pursuant to 37 C.F.R. §§ 1.933 and 1.555, VirnetX Inc., the patent owner, brings to the attention of the Examiner the documents listed on the attached PTO/SB/08 Form.

Copies of the listed U.S. patent documents are not enclosed. Copies of listed foreign patent documents and non-patent literature documents not previously submitted in a priority application—citation nos. C8, C19, C21, C24, and D257, D258, D259, D261, D263, D264, D266, and D292-D1219—are enclosed. *See* M.P.E.P. § 609.02(B)(2).

The patent owner respectfully requests that the Examiner consider the listed documents and indicate that they were considered by making appropriate notations on the attached form and returning the same to patent owner.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art." If the Examiner applies any of the documents as prior art against any claim in the instant proceeding and the patent owner determines that the cited documents do not constitute "prior art" under United States law, the patent owner reserves the right to present to the U.S. Patent and Trademark Office the relevant facts and law regarding the appropriate status of such documents.

The patent owner further reserves the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims in the instant proceeding.

If there is any fee due in connection with the filing of this paper, please charge the fee to Deposit Account 502624.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Dated: September 20, 2012

By: /Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
McDermott Will & Emery LLP
Attorney for Patent Owner

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com

Please recognize our Customer No. 23630 as our correspondence address.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A1	09/399,753	09/22/1998	Graig Miller et al.	
		A2	60/151,563	08/31/1999	Bryan Whittles	
		A3	60/134,547	05/17/1999	Victory Sheymov	
		A4	2,895,502	07/21/1959	Roper et al.	
		A5	4,761,334	08/1988	Sagoi et al.	
		A6	4,885,778	12/5/1989	Weiss, Kenneth	
		A7	4,920,484	4/24/1990	Ranade	
		A8	4,933,846	06/12/1990	Humphrey et al.	
		A9	4,952,930	08/28/1990	Franaszek et al.	
		A10	4,988,990	01/29/1991	Warrior	
		A11	5,164,988	11/17/1992	Matyas	
		A12	5,204,961	04/20/1993	Barlow	
		A13	5,276,735	01/04/1994	Boebert et al	
		A14	5,303,302	04/12/1994	Burrows	
		A15	5,311,593	05/10/1994	Carmi	
		A16	5,329,521	07/12/1994	Walsh et al.	
		A17	5,341,426	08/23/1994	Barney et al.	
		A18	5,367,643	11/22/1994	Chang et al	
		A19	5,384,848	01/24/1995	Kikuchi	
		A20	5,511,122	04/23/1996	Atkinson	
		A21	5,548,646	08/20/1996	Aziz et al.	
		A22	5,559,883	09/24/1996	Williams	
		A23	5,561,669	10/01/1996	Lenney et al	
		A24	5,588,060	12/24/1996	Aziz	
		A25	5,590,285	12/31/1996	Krause et al.	
		A26	5,625,626	04/29/1997	Umekita	
		A27	5,629,984	05/13/1997	McManis	
		A28	5,654,695	08/05/1997	Olnowich et al	
		A29	5,682,480	10/28/1997	Nakagawa	
		A30	5,689,566	11/18/1997	Nguyen	
		A31	5,689,641	11/18/1997	Ludwig et al.	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A32	5,740,375	04/14/1998	Dunne et al.	
		A33	5,757,925	05/1998	Faybishenko	
		A34	5,764,906	06/1998	Edelstein et al.	
		A35	5,771,239	06/23/1998	Moroney et al.	
		A36	5,774,660	6/30/1998	Brendel et al	
		A37	5,787,172	07/28/1998	Arnold	
		A38	5,790,548	08/04/1998	Sitaraman et al.	
		A39	5,796,942	08/18/1998	Esbensen	
		A40	5,805,801	09/08/1998	Holloway et al.	
		A41	5,805,803	09/08/1998	Birrell et al.	
		A42	5,822,434	10/13/1998	Caronni et al.	
		A43	5,842,040	11/24/1998	Hughes et al.	
		A44	5,845,091	12/01/1998	Dunne et al.	
		A45	5,864,666	01/1999	Shrader, Theodore Jack London	
		A46	5,867,650	02/02/1998	Osterman	
		A47	5,870,610	02/09/1999	Beyda et al.	
		A48	5,878,231	05/02/1999	Baehr et al	
		A49	5,892,903	04/06/1999	Klaus	
		A50	5,898,830	04/27/1999	Wesinger, Jr. et al.	
		A51	5,905,859	05/18/1999	Holloway et al.	
		A52	5,918,018	06/29/1999	Gooderum et al.	
		A53	5,918,019	06/29/1999	Valencia	
		A54	5,950,195	09/07/1999	Stockwell et al.	
		A55	5,950,519	09/14/1999	Anatoli	
		A56	5,960,204	09/28/1999	Yinger et al.	
		A57	5,996,016	11/30/1999	Thalheimer et al.	
		A58	6,006,259	12/21/1999	Adelman et al.	
		A59	6,006,272	12/21/1999	Aravamudan et al	
		A60	6,016,318	01/18/2000	Tomoike	
		A61	6,016,512	01/18/2000	Huitema	
		A62	6,041,342	03/21/2000	Yamaguchi	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	3	of	52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code *(if known)*			
		A63	6,052,788	04/2000	Wesinger et al.	
		A64	6,055,574	04/25/2000	Smorodinsky et al.	
		A65	6,061,346	05/2000	Nordman, Mikael	
		A66	6,061,736	05/09/2000	Rochberger et al	
		A67	6,079,020	06/20/2000	Liu	
		A68	6,081,900	06/2000	Subramaniam et al.	
		A69	6,092,200	07/18/2000	Muniyappa et al.	
		A70	6,101,182	08/2000	Sistanizadeh et al.	
		A71	6,119,171	09/12/2000	Alkhatib	
		A72	6,119,234	09/12/2000	Aziz et al.	
		A73	6,131,121	10/10/2000	Mattaway et al.	
		A74	6,147,976	11/14/2000	Shand et al.	
		A75	6,157,957	12/05/2000	Berthaud	
		A76	6,158,011	12/05/2000	Chen et al.	
		A77	6,168,409	01/02/2001	Fare	
		A78	6,173,399	01/09/2001	Gilbrech	
		A79	6,175,867	01/16/2001	Taghadoss	
		A80	6,178,409	01/23/2001	Weber et al.	
		A81	6,178,505	01/23/2001	Schneider et al	
		A82	6,179,102	01/30/2001	Weber, et al.	
		A83	6,182,141	1/30/2001	Blum et al.	
		A84	6,199,112	03/2001	Wilson, Stephen K.	
		A85	6,202,081	03/2001	Naudus, Stanley T.	
		A86	6,222,842	04/24/2001	Sasyan et al.	
		A87	6,223,287	04/24/2001	Douglas et al.	
		A88	6,226,748	05/01/2001	Bots et al.	
		A89	6,226,751	05/01/2001	Arrow et al..	
		A90	6,233,618	05/15/2001	Shannon	
		A91	6,243,360	06/05/2001	Basilico	
		A92	6,243,749	06/05/2001	Sitaraman et al.	
		A93	6,243,754	06/05/2001	Guerin et al	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO			
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
(Use as many sheets as necessary)		*Examiner Name*	Dennis G. Bonshock
Sheet 4	of 52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A94	6,246,670	06/12/2001	Karlsson et al.	
		A95	6,256,671	07/03/2001	Strentzsch et al.	
		A96	6,262,987	07/17/01	Mogul, Jeffrey C.	
		A97	6,263,445	07/17/2001	Blumenau	
		A98	6,269,099	07/31/2001	Borella et al.	
		A99	6,286,047	09/04/2001	Ramanathan et al	
		A100	6,298,341	10/02/01	Mann, et al.	
		A101	6,301,223	10/9/2001	Hrastar et al	
		A102	6,308,213	10/23/2001	Valencia	
		A103	6,308,274	10/23/2001	Swift	
		A104	6,311,207	10/30/2001	Mighdoll et al	
		A105	6,314,463	11/2001	Abbott et al.	
		A106	6,324,161	11/27/2001	Kirch	
		A107	6,330,562	12/11/2001	Boden et al.	
		A108	6,332,158	12/18/2001	Risley et al.	
		A109	6,333,272	12/25/01	McMillin, et al.	
		A110	6,338,082	01/08/02	Schneider, Eric	
		A111	6,353,614	03/05/2002	Borella et al.	
		A112	6,425,003	07/23/2002	Herzog et al.	
		A113	6,430,155	08/06/2002	Davie et al	
		A114	6,430,610	08/06/2002	Carter	
		A115	6,487,598	11/26/2002	Valencia	
		A116	6,496,867	12/17/2002	Beser et al.	
		A117	6,499,108	12/24/2002	Johnson	
		A118	6,502,135	12/2002	Munger et al.	
		A119	6,505,232	01/07/2003	Mighdoll et al	
		A120	6,510,154	01/21/2003	Mayes et al	
		A121	6,549,516	04/15/2003	Albert et al	
		A122	6,557,037	04/2003	Provino, Joseph E.	
		A123	6,560,634	05/06/2003	Broadhurst	
		A124	6,571,296	05/27/2002	Dillon	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	5	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A125	6,571,338	05/27/2003	Shaio et al.	
		A126	6,581,166	7/17/2003	Hirst et al.	
		A127	6,606,708	08/12/2003	Devine et al.	
		A128	6,615,357	9/2/2003	Boden et al.	
		A129	6,618,761	09/09/2003	Munger et al.	
		A130	6,671,702	12/30/2003	Kruglikov et al	
		A131	6,687,551	2/3/2004	Steindl	
		A132	6,687,746	02/03/04	Shuster, et al.	
		A133	6,701,437	03/02/2004	Hoke et al.	
		A134	6,714,970	3/30/2004	Fiveash et al.	
		A135	6,717,949	4/6/2004	Boden et al.	
		A136	6,751,738	06/15/2004	Wesinger, Jr. et al..	
		A137	6,752,166	06/22/04	Lull, et al.	
		A138	6,757,740	06/29/04	Parekh, et al.	
		A139	6,760,766	7/6/2004	Sahlqvist	
		A140	6,813,777	11/2004	Weinberger et al.	
		A141	6,826,616	11/30/2004	Larson et al.	
		A142	6,839,759	1/4/2005	Larson et al.	
		A143	6,937,597	08/30/2005	Rosenberg et al.	
		A144	7,010,604	3/7/2006	Munger et al.	
		A145	7,039,713	05/2006	Van Gunter et al.	
		A146	7,072,964	07/04/2006	Whittle et al.	
		A147	7,133,930	11/7/2006	Munger et al.	
		A148	7,167,904	01/23/07	Devarajan, et al.	
		A149	7,188,175	03/06/07	McKeeth, James A.	
		A150	7,188,180	3/6/2007	Larson et al.	
		A151	7,197,563	3/27/2007	Sheymov et al.	
		A152	7,353,841	04/08/08	Kono, et al.	
		A153	7,418,504	08/2008	Larson et al.	
		A154	7,461,334	12/02/08	Lu, et al.	
		A155	7,490,151	02/2009	Munger et al.	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	6	of	52	*Attorney Docket Number*	077580-0160

U.S. PATENTS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		A156	7,493,403	02/2009	Shull et al.	
		A157	7,584,500	09/2009	Dillon et al.	
		A158	7,764,231	07/27/2010	Karr et al.	
		A159	7,852,861	12/2010	Wu et al.	
		A160	7,921,211	04/2011	Larson et al.	
		A161	7,933,990	04/2011	Munger et al.	
		A162	8,051,181	11/2011	Larson et al.	

Note: Submission of copies of U.S. Patents and published U.S. Patent Applications is not required.

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	***Complete if Known***
	Control Number: 95/001,949
	Filing Date: March 28, 2012
	First Named Inventor: Victor Larson
	Art Unit: 3992
	Examiner Name: Dennis G. Bonshock
Sheet 7 of 52	*Attorney Docket Number*: 077580-0160

PUBLISHED U.S. PATENT APPLICATIONS

Tab No.	Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		B1	US2001/0049741	12/2001	Skene et al.	
		B2	US2002/0004898	1/10/02	Droge	
		B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
		B4	US2004/0199493	10/2004	Ruiz et al.	
		B5	US2004/0199520	10/2004	Ruiz et al.	
		B6	US2004/0199608	10/2004	Rechterman et al.	
		B7	US2004/0199620	10/2004	Ruiz et al.	
		B8	US2005/0055306	3/10/05	Miller et al.	
		B9	US2005/0108517	05/2005	Dillon et al.	
		B10	US2006/0059337	03/16/2006	Polyhonen et al.	
		B11	US2006/0123134	06/2006	Munger et al.	
		B12	US2007/0208869	09/2007	Adelman et al.	
		B13	US2007/0214284	09/2007	King et al.	
		B14	US2007/0266141	11/2007	Norton, Michael Anthony	
		B15	US2008/0005792	01/2008	*Larson et al.	
		B16	US2008/0144625	06/2008	Wu et al.	
		B17	US2008/0235507	09/2008	Ishikawa et al.	
		B18	US2009/0193498	07/2009	Agarwal et al.	
		B19	US2009/0193513	07/2009	Agarwal et al.	
		B20	US2009/0199258	08/2009	Deng et al.	
		B21	US2009/0199285	09/2009	Agarwal et al.	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	8	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

FOREIGN PATENT DOCUMENTS

Tab	Examiner Initials*	Cite No.	Foreign Patent Document Country Code Number Kind Code (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Translation
		C1	DE19924575	12/2/99	Provino et al.		
		C2	EP0814589	12/29/1997	AT&T Corp.		
		C3	EP0838930	4/29/1988	Digital Equipment Corporation		
		C4	EP0858189	8/12/98	Maciel et al.		
		C5	EP836306	4/15/1998	HEWLETT PACKARD CO		
		C6	GB2317792	04/01/1998	Secure Computing Corporation		
		C7	GB2334181	08/11/1999	NEC Technologies		
		C8	GB2340702	02/23/2000	Sun Microsystems Inc.		
		C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		
		C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		
		C11	JP10-070531	03/10/1998	Brother Ind Ltd.		
		C12	JP62-214744	9/21/1987	Hitachi Ltd.		
		C13	WO0070458	11/23/2000	Comsec Corporation		
		C14	WO0017775	3/30/00	Miller et al.		
		C15	WO01016766	03/08/2001	Science Applications International Corporation		
		C16	WO0150688	7/12/01	Kriens		
		C17	WO9827783	06/25/1998	Northern Telecom Limited		
		C18	WO9855930	12/10/98	Tang		
		C19	WO9843396	10/01/1998	Northern Telecom Limited		
		C20	WO9859470	12/30/98	Kanter et al.		
		C21	WO9911019	03/04/1999	V One Corp		
		C22	WO9938081	7/29/99	Paulsen et al.		
		C23	WO9948303	9/23/99	Cox et al.		
		C24	WO01/61922	02/12/2001	Science Application International Corporation		

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	9	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D4	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	D6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D8	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D9	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D10	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	D11	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	D12	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D13	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D14	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	D15	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D16	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D17	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	D18	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	D19	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	D20	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D21	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D22	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D23	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	10	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D24	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D25	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	D26	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D27	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conference on Communications architectures & protocols. pp. 84-91, ACM Press, NY, NY 1986.	
	D28	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D29	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	D30	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation.	
	D31	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D32	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D33	I. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) RFC1101, DNS SRV)	
	D34	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	D35	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	D37	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	D38	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	D39	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	D40	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	D41	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	D42	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	D43	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	
	D44	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	11	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D45	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	D46	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	D47	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista)	
	D48	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	D49	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	D50	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)	
	D51	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/199706200300312/www.aventail.com/educate/whitepaper/ipmw.html (1997). (Corporate Access, Aventail)	
	D53	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	D54	Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschtag I, Onion Routing)	
	D55	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	D62	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	D63	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	D64	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	12	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D65	Automotive Industry Action Group, “ANXO Certification Authority Service and Directory Service Definition for ANX Release 1,” AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Definition, ANX)	
	D66	Automotive Industry Action Group, “ANXO Certification Process and ANX Registration Process Definition for ANX Release 1,” AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	D67	Aventail Corp., “Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols,” June 2, 1997. (First VPN, Aventail)	
	D68	Syverson, et al. “Private Web Browsing,” Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	D69	Bellcore, “Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1,” AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	D70	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	D71	R. Atkinson, “Key Exchange Delegation Record for the DNS,” Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	D72	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	D73	1998 Microsoft Professional Developers Conference DVD (“1998 PDC DVD-ROM”) (including screenshots captured there from and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	D74	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (*available at* http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue). (NT Beta, Microsoft Prior Art VPN Technology)	
	D76	“What ports does SSL use” *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	D77	Aventail Corp., “Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple,” Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	D78	R. G. Moskowitz, “Network Address Translation Issues with IPsec,” Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	D79	H. Schulzrinne, et al, “Internet Telephony Gateway Location,” Proceedings of IEEE INfocom ‘98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	D80	C. Huitema, 45 al. “Simple Gateway Control Protocol,” Version 1.0 (May 5, 1998). (SGCP)	
	D81	DISA “Secret Internet Protocol Router Network,” SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). DISA, SIPRNET)	
	D82	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	D83	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	13	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D84	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	D85	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	D86	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	D87	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	D88	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	D89	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	D90	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	D91	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	D92	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	D93	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	D94	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	D95	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	D96	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	D97	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	D98	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	D99	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*,<draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). Scott VPNs)	
	D101	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	D102	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	D103	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	D104	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	D105	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	14	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D106	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	D107	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	D108	Bhattacharya, et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	D109	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	D110	Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D111	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	D112	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	D113	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	D114	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	D115	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	D116	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	D117	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	D118	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	D119	Assured Digital Products. (Assured Digital)	
	D120	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	D121	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	D122	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	D123	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	D124	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	D125	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	
	D126	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	D127	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	D128	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	D129	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	D130	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	D131	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 15	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D132	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	D140	Dan Sterne *et al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	D142	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	D143	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	D144	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	D145	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D147	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D148	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D149	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	16	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D150	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	D162	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/techneUarchive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	D165	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	D168	Kenneth Gregg, *et al., Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/enus/library/bb545687(VS.85.printer).aspx (Remote Access)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	17	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D170	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D171	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D172	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch0l.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D175	F-Secure, *F-Secure NameSurfer*(May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) F-Secure VPN 3)	
	D177	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	D185	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	18	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D187	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	D189	F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., *SafeNet/Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	D198	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	D204	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	D205	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	D206	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	D207	Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0* (September 21, 1998)	
	D209	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	D210	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	D211	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	D212	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	D213	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	D214	*Virtual Private Network Demonstration* (March 21, 1998)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO			
INFORMATION DISCLOSURE STATEMENT BY APPLICANT			
(Use as many sheets as necessary)			
Sheet	19	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D215	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	D216	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	D217	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	D218	Information Assurance, *Science Fair Agenda* (2000)	
	D219	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	D220	*IFE 3.1 Technology Dependencies* (2000)	
	D221	*IFE 3.1 Topology* (February 9, 2000)	
	D222	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	D224	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	D225	Information Assurance/NAI Labs, Dynamic Virtual Private Networks Presentation v.3 (2000)	
	D226	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	D228	Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, *MCSE Test Success: Proxy Server 2*(1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D238	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	D239	*AutoSOCKS v2. 1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers, 1 99x/msg00945.html	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	20	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D241	FirstVPN Enterprise Networks, Overview	
	D242	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	D243	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	D244	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	D245	Virtual Private Networks - Assured Digital Incorporated - ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	D246	Accessware - The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	D247	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	D248	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	D250	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, “Building and Managing Virtual Private Networks” (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, “A novel scheme combining interleaving technique with cipher in Rayleigh fading channels,” Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
	D256	Davies and Price, edited by Tadahiro Uezono, “Network Security”, Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
	D257	Davies et al., “An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,” Security for Computer Networks, Second Edition, pp. 98-101 (1989)	
	D258	Baumgartner et al, “Differentiated Services: A New Approach for Quality of Service in the Internet,” International Conference on High Performance Networking, 255-273 (1998)	
	D259	Chapman et al., “Domain Name System (DNS),” 278-296 (1995)	
	D260	Davila et al., “Implementation of Virtual Private Networks at the Transport Layer,” M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D261	De Raadt et al., “Cryptography in OpenBSD,” 9 pages (1999)	
	D262	Eastlake, “Domain Name System Security Extensions,” Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	
	D263	Gunter et al., “An Architecture for Managing QoS-Enabled VRNs Over the Internet,” Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	21	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D264	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D265	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D266	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	D267	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	
	D268	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	D269	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D270	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D271	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D272	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D273	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	22	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages.	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages.	
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages.	
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	
	D299	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	
	D300	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D301	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D302	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D303	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D304	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D305	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D306	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D307	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	23	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D308	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D309	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D310	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D311	Tannenbaum, "Computer Networks," pages 202-219 (1996)	
	D312	Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D315	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D317	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D318	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D319	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D320	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D321	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D322	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D323	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D324	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D325	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D326	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent.	
	D327	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D328	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D329	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D330	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D331	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D332	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D333	Exhibit 19, RFC 2595 vs. Claims of the '211 Patent	
	D334	Exhibit 20, RFC 2595 vs. Claims of the '504 Patent	
	D335	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D336	Exhibit 22, iPASS vs. Claims of the '211 Patent	
	D337	Exhibit 23, iPASS vs. Claims of the '504 Patent	
	D338	Exhibit 24, "US '034" vs. Claims of the '135 Patent	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034") vs. Claims of the '211 Patent	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034") vs. Claims of the '504 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	24	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D341	Exhibit 27, US '287 vs. Claims of the '135 Patent	
	D342	Exhibit 28, US '287 vs. Claims of the '211 Patent	
	D343	Exhibit 29, US '287 vs. Claims of the '504 Patent	
	D344	Exhibit 30, Overview of Access VPNs vs. Claims of the '135 Patent	
	D345	Exhibit 31, Overview of Access VPNs vs. Claims of the '211 Patent	
	D346	Exhibit 32, Overview of Access VPNs vs. Claims of the '504 Patent	
	D347	Exhibit 34, RFC 1928 vs. Claims of the '135 Patent	
	D348	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D349	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D350	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D351	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D352	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D353	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D354	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D355	Exhibit 42,SecureConnect vs. Claims of the '504 Patent	
	D356	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D357	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D358	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D359	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D360	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D361	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D362	Exhibit 49, US '132 vs. Claims of the '135 Patent	
	D363	Exhibit 50, US '132 vs. Claims of the '211 Patent	
	D364	Exhibit 51, US '132 vs. Claims of the '504 Patent	
	D365	Exhibit 52, US '213 vs. Claims of the '135 Patent	
	D366	Exhibit 53, US '213 vs. Claims of the '211 Patent	
	D367	Exhibit 54, US '213 vs. Claims of the '504 Patent	
	D368	Exhibit 55, B&M VPNs vs. Claims of the '135 Patent	
	D369	Exhibit 56, B&M VPNs vs. Claims of the '211 Patent	
	D370	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D371	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D372	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D373	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D374	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D375	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D376	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D377	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D378	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	25	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D379	Exhibit 66, RFC 2401 vs. Claims of the ’504 Patent	
	D380	Exhibit 67, RFC 2486 vs. Claims of the ’135 Patent	
	D381	Exhibit 68, RFC 2486 vs. Claims of the ’211 Patent	
	D382	Exhibit 69, RFC 2486 vs. Claims of the ’504 Patent	
	D383	Exhibit 70, Understanding IPSec vs. Claims of the ’135 Patent	
	D384	Exhibit 71, Understanding IPSec vs. Claims of the ’211 Patent	
	D385	Exhibit 72, Understanding IPSec vs. Claims of the ’504 Patent	
	D386	Exhibit 73, US ‘820 vs. Claims of the ’135 Patent	
	D387	Exhibit 74, US ‘820 vs. Claims of the ’211 Patent	
	D388	Exhibit 75, US ‘820 vs. Claims of the ’504 Patent	
	D389	Exhibit 76, US ‘019 vs. Claims of the ’211 Patent	
	D390	Exhibit 77, US ‘019 vs. Claims of the ’504 Patent	
	D391	Exhibit 78, US ‘049 vs. Claims of the ’135 Patent	
	D392	Exhibit 79, US ‘049 vs. Claims of the ’211 Patent	
	D393	Exhibit 80, US ‘049 vs. Claims of the ’504 Patent	
	D394	Exhibit 81, US ‘748 vs. Claims of the ’135 Patent	
	D395	Exhibit 82, US ‘261 vs. Claims of the ’135 Patent	
	D396	Exhibit 83, US ‘261 vs. Claims of the ’211 Patent	
	D397	Exhibit 84, US ‘261 vs. Claims of the ’504 Patent	
	D398	Exhibit 85, US ‘900 vs. Claims of the ’135 Patent	
	D399	Exhibit 86, US ‘900 vs. Claims of the ’211 Patent	
	D400	Exhibit 87, US ‘900 vs. Claims of the ’504 Patent	
	D401	Exhibit 88, US ‘671 vs. Claims of the ’135 Patent	
	D402	Exhibit 89, US ‘671 vs. Claims of the ’211 Patent	
	D403	Exhibit 90, US ‘671 vs. Claims of the ’504 Patent	
	D404	Exhibit 91, JP ‘704 vs. Claims of the ’135 Patent	
	D405	Exhibit 92, JP ‘704 vs. Claims of the ’211 Patent	
	D406	Exhibit 93, JP ‘704 vs. Claims of the ’504 Patent	
	D407	Exhibit 94, GB ‘841 vs. Claims of the ’135 Patent	
	D408	Exhibit 95, GB ‘841 vs. Claims of the ’211 Patent	
	D409	Exhibit 96, GB ‘841 vs. Claims of the ’504 Patent	
	D410	Exhibit 97, US ‘318 vs. Claims of the ’135 Patent	
	D411	Exhibit 98, US ‘318 vs. Claims of the ’211 Patent	
	D412	Exhibit 99, US ‘318 vs. Claims of the ’504 Patent	
	D413	Exhibit 100, VPN/VLAN vs. Claims of the ’135 Patent	
	D414	Exhibit 101, Nikkei vs. Claims of the ’135 Patent	
	D415	Exhibit 102, NIKKEI vs. Claims of the ’211 Patent	
	D416	Exhibit 103, NIKKEI vs. Claims of the ’504 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	26	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D417	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D418	Exhibit 105, Omron vs. Claims of the '135 Patent	
	D419	Exhibit 106, Gauntlet System vs. Claims of the '135 Patent	
	D420	Exhibit 107, Gauntlet System vs. Claims of the '151 Patent	
	D421	Exhibit 108, Gauntlet System vs. Claims of the '180 Patent	
	D422	Exhibit 109, Gauntlet System vs. Claims of the '211 Patent	
	D423	Exhibit 110, Gauntlet System vs. Claims of the '504 Patent	
	D424	Exhibit 111, Gauntlet System vs. Claims of the '759 Patent	
	D425	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D426	Exhibit 113, IntraPort System vs. Claims of the '151 Patent	
	D427	Exhibit 114, IntraPort System vs. Claims of the '180 Patent	
	D428	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D429	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D430	Exhibit 117, IntraPort System vs. Claims of the '759 Patent	
	D431	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D432	Exhibit 119, Altiga VPN System vs. Claims of the '151 Patent	
	D433	Exhibit 120, Altiga VPN System vs. Claims of the '180 Patent	
	D434	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D435	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D436	Exhibit 123, Altiga VPN System vs. Claims of the '759 Patent	
	D437	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D438	Exhibit 125, Kiuchi vs. Claims of the '151 Patent	
	D439	Exhibit 126, Kiuchi vs. Claims of the '180 Patent	
	D440	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D441	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D442	Exhibit 129, Kiuchi vs. Claims of the '759 Patent	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '151 Patent	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '180 Patent	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D448	Exhibit 135, Overview vs. Claims of the '759 Patent	
	D449	Exhibit 136, RFC 2401 vs. Claims of the '759 Patent	
	D450	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	27	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D451	Exhibit 138, Schulzrinne vs. Claims of the '151 Patent	
	D452	Exhibit 139, Schulzrinne vs. Claims of the '180 Patent	
	D453	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D454	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D455	Exhibit 142, Schulzrinne vs. Claims of the '759 Patent	
	D456	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D457	Exhibit 144, Solana vs. Claims of the '151 Patent	
	D458	Exhibit 145, Solana vs. Claims of the '180 Patent	
	D459	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D460	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D461	Exhibit 148, Solana vs. Claims of the '759 Patent	
	D462	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D463	Exhibit 150, Atkinson vs. Claims of the '151 Patent	
	D464	Exhibit 151, Atkinson vs. Claims of the '180 Patent	
	D465	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D466	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D467	Exhibit 154, Atkinson vs. Claims of the '759 Patent	
	D468	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D469	Exhibit 156, Marino vs. Claims of the '151 Patent	
	D470	Exhibit 157, Marino vs. Claims of the '180 Patent	
	D471	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D472	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D473	Exhibit 160, Marino vs. Claims of the '759 Patent	
	D474	Exhibit 161, Aziz ('646) vs. Claims of the '759 Patent	
	D475	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D476	Exhibit 163, Wesinger vs. Claims of the '151 Patent	
	D477	Exhibit 164, Wesinger vs. Claims of the '180 Patent	
	D478	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D479	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D480	Exhibit 167, Wesinger vs. Claims of the '759 Patent	
	D481	Exhibit 168, Aziz ('234) vs. Claims of the '135 Patent	
	D482	Exhibit 169, Aziz ('234) vs. Claims of the '151 Patent	
	D483	Exhibit 170, Aziz ('234) vs. Claims of the '180 Patent	
	D484	Exhibit 171, Aziz ('234) vs. Claims of the '211 Patent	
	D485	Exhibit 172, Aziz ('234) vs. Claims of the '504 Patent	
	D486	Exhibit 173, Aziz ('234) vs. Claims of the '759 Patent	
	D487	Exhibit 174, Schneider vs. Claims of the '759 Patent	
	D488	Exhibit 175, Valencia vs. Claims of the '135 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	28	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D489	Exhibit 176, Valencia vs. Claims of the '151 Patent	
	D490	Exhibit 177, Valencia vs. Claims of the '180 Patent	
	D491	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D492	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867 vs. Claims of the '180 Patent	
	D494	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D495	Exhibit 182, Davison vs. Claims of the '151 Patent	
	D496	Exhibit 183, Davison vs. Claims of the '180 Patent	
	D497	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D498	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D499	Exhibit 186, Davison vs. Claims of the '759 Patent	
	D500	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D501	Exhibit 188, AutoSOCKS v2.1 vs. Claims of the '151 Patent	
	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide vs. Claims of the '180 Patent	
	D503	Exhibit 190, AutoSOCKS vs. Claims of the '759 Patent	
	D504	Exhibit 191, Aventail Connect 3.01/2.51 vs. Claims of the '135 Patent	
	D505	Exhibit 192, Aventail Connect v3.01/2.51 vs. Claims of the '151 Patent	
	D506	Exhibit 193, Aventail Connect 3.01/2.51 vs. Claims of the '180 Patent	
	D507	Exhibit 194, Aventail Connect 3.01/2.51 vs. Claims of the '759 Patent	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '135 Patent	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '151 Patent	
	D510	Exhibit 197, Aventail Connect 3.1/2.6 vs. Claims of the '180 Patent	
	D511	Exhibit 198, Aventail Connect 3.1/2.6 vs. Claims of the '759 Patent	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '151 Patent	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 Patent	
	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D517	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D518	Exhibit 205, Domain Name System (DNS) Security vs. Claims of the '504 Patent	
	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	29	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '135 Patent	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '151 Patent	
	D528	Exhibit 215, U.S. Patent No. 6,643,701 vs. Claims of the '135 Patent	
	D529	Exhibit 216, U.S. Patent No. 6,643,701 vs. Claims of the '151 Patent	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '151 Patent	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '135 Patent	
	D532	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D533	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '151 Patent	
	D535	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D536	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '151 Patent	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System vs. Claims of the '759 Patent	
	D546	Exhibit A: Copy of U.S. Patent No. 6,502,135	
	D547	Exhibit A: Copy of U.S. Patent No. 7,490,151	
	D548	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D549	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D550	Exhibit B-1: File History of U.S. Patent 6,502,135	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	30	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D551	Exhibit B-2: Reexamination Record No. 95/001,269	
	D552	Exhibit C1: Claim Chart – Aventail Connect v3.1 (Patent No. 6,502,135)	
	D553	Exhibit C2: Claim Chart Aventail Connect V3.01 (Patent No. 6,502,135)	
	D554	Exhibit C-1: Copy of U.S. Patent No. 7,010,604	
	D555	Exhibit C2: Claim Chart Aventail Autosocks (Patent No. 7,490,151)	
	D556	Exhibit C1: Claim Chart Aventail Connect v3.01 (Patent No. 7,490,151)	
	D557	Exhibit C-2: Provisional Application 60/106,261	
	D558	Exhibit C3: Claim Chart Aventail AutoSOCKS (Patent No. 6,502,135)	
	D559	Exhibit C3: Claim Chart BinGO (Patent No. 7,490,151)	
	D560	Exhibit C-3: Provisional Application 60/137,704	
	D561	Exhibit C4: Claim Chart Wang (Patent No. 6,502,135)	
	D562	Exhibit C4: Claim Chart Beser (Patent No. 7,490,151)	
	D563	Exhibit C5: Claim Chart Beser (Patent No. 6,502,135)	
	D564	Exhibit C5: Claim Chart Wang (Patent No. 7,490,151)	
	D565	Exhibit C6: Claim Chart BinGO (Patent No. 6,502,135)	
	D566	Exhibit D: Memorandum Opinion in *VirnetX v. Microsoft.*	
	D567	Exhibit D-1: Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HPPT-Based Network on the Internet," Published in the Proceedings of SNDSS 1996.	
	D568	Exhibit D-10: D.E. Denning and G.M. Sacco, "Time-stamps in Key Distribution Protocols," Communications of the ACM, Vol. 24, N.8, pp. 533-536. August 1981.	
	D569	Exhibit D-11: C.I. Dalton and J.F. Griffin, "Applying Military Grade Security to the Internet," Proceedings of the 8th Joint European Networking Conference (JENC 8), (May 12-15 1997).	
	D570	Exhibit D-12: Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based protocols Secure against Dictionary Attacks," 1992 IEEE Symposium on Security and Privacy (1992).	
	D571	Exhibit D-2: Copy of U.S. Pat. No. 5,898,830	
	D572	Exhibit D-3: Eduardo Solana and Jürgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains," Security Protocols Workshop 1997, pp. 37-51.	
	D573	Exhibit D-4: Copy of U.S. Pat. No. 6,119,234	
	D574	Exhibit D-5: Jeff Sedayao, "Mosaic Will Kill My Network!' – Studying Network Traffic Patterns of Mosaic Use," in Electron. Proc. 2nd World Wide Web Conf. '94: Mosaic and the Web, Chicago, IL, Oct. 1994.	
	D575	Exhibit D-6: M. Luby Juels and R. Ostrovsky, "Security of Blind Digital Signatures," Crypto '97, LNCS 1294, pages 150-164, Springer-Verlag, Berlin, 1997.	
	D576	Exhibit D-8: David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).	
	D577	Exhibit D-9: Copy of U.S. Pat. No. 7,764,231	
	D578	Exhibit E-1: Claim Charts Applying Kiuchi and Other References to Claims of the '135 Patent.	
	D579	Exhibit E1: Declaration of Chris Hopen (Patent No. 6,502,135)	
	D580	Exhibit E1: Declaration of Chris Hopen (Patent No. 7,490,151)	
	D581	Exhibit E-2: Claim Charts Applying Wesinger and Other References to Claims of the '135 Patent.	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	31	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D582	Exhibit E2: Declaration of Michael Fratto (Patent No. 6,502,135)	
	D583	Exhibit E2: Declaration of Michael Fratto (Patent No. 7,490,151)	
	D584	Exhibit E-3: Claim Charts Applying Solana and Other References to Claims of the ’135 Patent.	
	D585	Exhibit E3: Declaration of James Chester (Patent No. 6,502,135)	
	D586	Exhibit E3: Declaration of James Chester (Patent No. 7,490,151)	
	D587	Exhibit E-4: Claim Charts Applying Aziz and Other References to Claims of the ’135 Patent.	
	D588	Exhibit X1: Aventail Connect Administrator’s Guide v3.1/v2.6., PP 1-20 (1996-1999)	
	D589	Exhibit X10: Copy of U.S. Patent No. 4,885,778	
	D590	Exhibit X11: Copy of U.S. Patent No. 6,615,357	
	D591	Exhibit X2: Aventail Connect Administrator’s Guide v3.01/v2.51., PP 1-116 (1996-1999)	
	D592	Exhibit X3: Aventail AutoSOCKS Administration & User’s Guide v2.1., PP 1-70 (1996-1999)	
	D593	Exhibit X4: Reed et al., ”Proxies for Anonymous Routine,” 12th Annuary Computer Security Applications Conference, San Diego, CA, December -9-13, pp 1-10 (1996).	
	D594	Exhibit X5: Wang, The Broadband Forum Technical Report, “TR-025 – Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL,” Issue 1.0; pp. 1-24 , v1.0 (1999).	
	D595	Exhibit X6: Copy of U.S. Patent No. 6,496,867	
	D596	Exhibit X7: BinGO! User’s Guide Incorporating by Reference BinGO! Extended Feature Reference.	
	D597	Exhibit X7: Kent et al., “Security Architecture for the Internet Protocol, “ Network Working Group Request for Comments (RFC) 2401, pp 1-70 (1998).	
	D598	Exhibit X8: Copy of U.S. Patent No. 6,182,141	
	D599	Exhibit X9: BinGO! User’s Guide v1.6 (1999).	
	D600	Exhibit Y1: Aventail Extranet Server 3.0 Administrator’s Guide.	
	D601	Exhibit Y10: Hanks, S., et al., RFC1701, “Generic Routing Encapsulation (GRE),” 1994, Is Accessbile at http://www.ietf.org/rfc/rfc1701.txt.	
	D602	Exhibit Y10: Socolofsky, T. et al., RFC 1180, “A TCP/IP Tutorial,” January 1991.	
	D603	Exhibit Y11: Simpson, W., editor, RFC 1661, “The Point-to-Point Protocol (PPP),” July 1994.	
	D604	Exhibit Y11: Simpson, W., RFC1994, “PPP Challenge Handshake Authentication Protocol (CHAP),” 1996, http://www.ietf.org/rdc/rfc1994.txt.	
	D605	Exhibit Y12: Meyer, G., RFC 1968, “The PPP Encryption Control Protocol (ECP),” June 1996.	
	D606	Exhibit Y12: Perkins, D., RFC1171, “The Point-To-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-To-Point Links,” 1990, Is Accessible at http://www.ietf.org/rfc/rfc1171.txt.	
	D607	Exhibit Y13: Kummert, H., RFC 2420, “The PPP Triple-DES Encryption Protocol (3DESE),” September, 1998.	
	D608	Exhibit Y14: Townsley, W.M., et al., RFC 2661, “Layer Two Tunneling Protocol ‘L2TP’,” August 1999.	
	D609	Exhibit Y15: Pall, G.S., RFC 2118, “Microsoft Point-To-Point Encryption (MPPE) Protocol,” March 1997.	
	D610	Exhibit Y16: Gross, G., et al., RFC 2364, “PPP Over AAL5,” July 1998.	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	32	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D611	Exhibit Y17: Srisuresh, P., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999.	
	D612	Exhibit Y18: Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993.	
	D613	Exhibit Y2: Goldschlag et al., "Hiding Routing Information" (1996).	
	D614	Exhibit Y3: Copy of U.S. Patent No. 5,950,519	
	D615	Exhibit Y4: Ferguson, P. and Huston, G., "What Is a VPN", The Internet Protocol Journal, Vol 1., No. 1 (June 1998 ("Ferguson").	
	D616	Exhibit Y5: Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC1034").	
	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodburn, R.A., et al., RFC1241, "A Scheme for an Internet Encapsulation Protocol: Version 1," 1991.	
	D620	Exhibit Y9: Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996.	
	D621	Exhibit Y9: Simpson, W., RFC1853, "IP in IP Tunneling," 1995, Is Accessible at http://ww.ietf.org/rfc/rfc1583.txt.	
	D622	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 6,502,135)	
	D623	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 7,490,151)	
	D624	Request for Inter Partes Reexamination (Patent No. 6,502,135)	
	D625	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 6,502,135)	
	D626	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 7,490,151)	
	D627	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D628	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D629	Transmittal Letter (Patent No. 6,502,135)	
	D630	Transmittal Letter (Patent No. 7,490,151)	
	D631	Joint Claim Construction and Prehearing Statement	
	D632	Exhibit A: Agreed Upon Terms; P.R. 4-3 Joint Claims Construction and Prehearing Statement	
	D633	Exhibit B: Disputed Claim Terms; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D634	Exhibit C; VirnetX's Proposed Construction of Claim Terms and Supporting Evidence	
	D635	Exhibit D; Defendants' Intrinsic and Extrinsic Support; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D636	U.S. Patent 6,839,759	
	D637	Exhibit B-4; VirnetX, Inc. v. Microsoft Corp., Case No. 6:07-cv-80, Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759 (E.D. Tex. Dec. 18, 2009)	
	D638	Exhibit D-2; Kent et al., "Security Architecture for the Internet Protocol," Internet Engineering Task Force, Internet Draft, (Feb. 1998)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		**Complete if Known**	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 33	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D639	Exhibit D-3; Aziz et al., U.S. Patent 5,548,646 to Aziz et al., "System for Signatureless Transmission and Reception of Data Packets Between Computer Networks," Filed Sept. 15, 1994 and issued Aug. 20, 1996	
	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Internet Protocol," DARPA Internet Program Specification RFC 791 (Sept. 1981)	
	D644	Exhibit D-14; Caronni et al., "SKIP – Securing the Internet," 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '96) (June 19-21, 1996)	
	D645	Exhibit D-15; Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP), " IPSEC Work Group Draft (July 26, 1997)	
	D646	Exhibit E-1; Claim Charts Applying Kiuchi as a Primary Reference to the '759 Patent.	
	D647	Exhibit E-2; Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D648	Exhibit E-3; Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D649	Exhibit E-4; Claim Charts Applying Kent in view of Caronni as a Primary Combination of References to the '759 Patent	
	D650	Exhibit D-5; Edwards et al., "High Security Web Servers and Gateways," Computer Networks and ISDN System 29, pages 927-938 (Sept. 1997)	
	D651	Exhibit D-10; Lee et al., "Hypertext Transfer Protocol – HTTP/1.0," RFC 1945 (May 1996)	
	D652	Exhibit E-3; Claim Charts Applying Blum to Claims of the '151 Patent	
	D653	Exhibit B-1, File History of U.S. Patent 7,490,151	
	D654	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D655	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D656	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D657	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D658	VirnetX Inc., V. Mitel Networks Corp.; Defendants' Joint Invalidity Contentions	
	D659	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D660	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D661	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D662	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D663	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D664	Exhibit 42, SecureConnect vs. Claims of the '504 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO		***Complete if Known***	
		Control Number	95/001,949
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		*Filing Date*	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
(Use as many sheets as necessary)		*Examiner Name*	Dennis G. Bonshock
Sheet 34	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D665	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D666	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D667	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D668	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D669	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D670	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D671	Exhibit 49, Chuah vs. Claims of the '135 Patent	
	D672	Exhibit 50, Chuah vs. Claims of the '211 Patent	
	D673	Exhibit 51, Chuah vs. Claims of the '504 Patent	
	D674	Exhibit 52, U.S. '648 vs. Claims of the '135 Patent	
	D675	Exhibit 53, U.S. '648 vs. Claims of the '211 Patent	
	D676	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D677	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D678	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D679	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D680	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D681	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D682	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D683	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D684	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D685	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D686	Exhibit 67, US '072 vs. Claims of the '135 Patent	
	D687	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D688	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D689	Exhibit 70 Understanding IPSec vs. Claims of the '135 Patent	
	D690	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D691	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D692	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D693	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D694	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D695	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D696	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D697	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D698	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D699	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D700	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D701	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D702	Exhibit 83, US '261 vs. Claims of the '211 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				***Complete if Known***	
				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	35	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D703	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D704	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D705	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D706	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D707	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D708	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D709	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D710	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D711	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D712	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D713	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D714	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D715	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D716	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D717	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D718	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D719	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D720	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D721	Exhibit 102, Nikkei vs. Claims of the '211 Patent	
	D722	Exhibit 103, Nikkei vs. Claims of the '504 Patent	
	D723	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D724	Exhibit 106-A, Gauntlet System vs. Claims of the '135 Patent	
	D725	Exhibit 109-A, Gauntlet System vs. Claims of the '211 Patent	
	D726	Exhibit 110-A, Gauntlet System vs. Claims of the '504 Patent	
	D727	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D728	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D729	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D730	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D731	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D732	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D733	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D734	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D735	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D736	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D737	Exhibit 137, Schulzrinne vs. Claims of the '135 (Final) Patent	
	D738	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D739	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D740	Exhibit 143, Solana vs. Claims of the '135 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	36	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D741	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D742	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D743	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D744	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D745	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D746	Exhibit 168, Aziz vs. Claims of the '135 Patent	
	D747	Exhibit 171, U.S. '234 vs. Claims of the '211 Patent	
	D748	Exhibit 172, Aziz vs. Claims of the '504 Patent	
	D749	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D750	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D751	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D752	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D753	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D754	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP' vs. Claims of the '135 Patent	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401' vs. Claims of the '135 Patent	
	D763	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D764	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D765	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D766	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D768	Exhibit 228, U.S. 588 vs. Claims of the '211 Patent (Final)	
	D769	Exhibit 229, U.S. 588 vs. Claims of the '504 Patent (Final)	
	D770	Exhibit 230, Microsoft VPN vs. Claims of the '135 Patent (Final)	
	D771	Exhibit 231, Microsoft VPN vs. Claims of the '211 Patent (Final)	
	D772	Exhibit XX, Microsoft VPN vs. Claims of the '504 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	37	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D773	Exhibit Cisco-1, Cisco's Prior Art System vs. Claims of the '135 Patent	
	D774	Exhibit Cisco-4, Cisco's Prior Art System vs. Claims of the '211 Patent	
	D775	Exhibit Cisco-5, Cisco's Prior Art System vs. Claims of the '504 Patent	
	D776	Exhibit 225, US '037 vs. Claims of the '135 Patent	
	D777	Exhibit 226, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D778	Exhibit 227, US '393 vs. Claims of the '135 Patent	
	D779	Exhibit 233, The Miller Application vs. Claim 13 of the '135 Patent	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '504 Patent	
	D781	Exhibit 235, Microsoft VPN vs. Claims of the '504 Patent	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '211 Patent	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '504 Patent	
	D784	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D785	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D786	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D787	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D788	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D789	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D790	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D791	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D792	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D793	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent	
	D794	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D795	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D796	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D797	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D798	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D799	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D800	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D801	Exhibit 22, iPass vs. Claims of the '211 Patent	
	D802	Exhibit 23, iPass vs. Claims of the '504 Patent	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ("034 Patent") vs. Claims of the '135 Patent	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ("034 Patent") vs. Claims of the '211 Patent	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ("034 Patent") vs. Claims of the '504 Patent	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the '135 Patent	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the '211 Patent	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the '504 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	38	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D809	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D810	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D811	Exhibit 106, Gaunlet System and Gaunlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gaunlet System and Gaunlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gaunlet System vs. Claims of the '504 Patent	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D817	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D818	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D819	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D820	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D821	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D822	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D823	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect") vs. Claims of the '135 Patent	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '135 Patent	
	D826	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D827	Exhibit 205, Domain Name System (DNS) Security ("DNS Security") vs. Claims of the '504 Patent	
	D828	Exhibit 210, Lendenmann vs. Claims of the '211 Patent	
	D829	Exhibit 211, Lendenmann vs. Claims of the '504 Patent	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D831	Exhibit 215, Aziz vs. Claims of the '135 Patent	
	D832	Cisco '180, Efiling Acknowledgment	
	D833	Exhibit A, U.S. Patent 7,188,180	
	D834	Exhibit B1, File History of U.S. Patent 7,188,180	
	D835	Exhibit B2, File History of U.S. Patent Application No. 09/588,209	
	D836	Exhibit B3, File History of Reexamination Control No. 95/001,270, Reexamination of U.S. 7,188,180 requested by Microsoft Corp	
	D837	Exhibit D1, "Lendenmann": Rolf Lendenman, Understanding OSF DCE 1.1 For AIX and OS/2, IBM International Technical Support Organization (Oct. 1995).	
	D838	Exhibit D5, "Schneier": Bruce Schneier, Applied Cryptography (1996)	
	D839	Exhibit D6, RFC 793; Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Specification RFC 793 (Sept. 1981)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO		**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		*Control Number*	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
(Use as many sheets as necessary)		*Examiner Name*	Dennis G. Bonshock
Sheet 39	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	
	D841	Exhibit D8, "Rosenberry"; Ward Rosenberry, David Kenney, and Gerry Fisher, Understanding DCE (1993)	
	D842	Exhibit D9, Masys; Daniel R. Masys & Dixie B. Baker, "Protecting Clinical Data on Web Client Computers: The PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, Florida (Nov. 7-11, 1998)	
	D843	Exhibit E1, Claim Charts Applying Lendenmann as a Primary Reference to the '180 Patent.	
	D844	Exhibit E2, Claim Charts Applying Kiuchi as a Primary Reference to the '180 Patent	
	D845	Exhibit E3, Claim Charts Applying Solana as a Primary Reference to the '180 Patent	
	D846	Exhibit E4, Claim Charts Applying Schimpf and Rosenberry as a Primary Reference to the '180 Patent	
	D847	Request for Inter Partes Reexamination of Patent No. 7,188,180	
	D848	Modified PTO Form 1449	
	D849	Request for Inter Partes Reexamination Transmittal Form No. 7,188,180	
	D850	Exhibit A; U.S. Patent 7,921,211 with Terminal Disclaimer	
	D851	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,921,211)	
	D852	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D853	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D854	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser)	
	D855	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D856	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D857	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D858	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D859	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D860	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D861	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D862	Exhibit X1, Solana, E. et al. "Flexible Internet Secure Transactions Based on Collaborative Domains"	
	D863	Exhibit X2, U.S. Patent 6,557,037	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	40	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D864	Exhibit X4, Atkinson, R., IETF RFC 2230, "Key Exchange Delegation Record for the DNS" (November 1997)	
	D865	Exhibit X6, Kent, et al., IETF RFC 2401, "Security Architecture for the Internet Protocol" (November 1998) Is Accessible at: http://www.ietf.org/rfc/rfc2401.txt	
	D866	Exhibit X7, Eastlake, D. et al., IETF RFC 2065, "Domain Name System Security Extensions" (January 1997) Is Accessible at: http://www.ietf.org/rfc/rfc2065.txt	
	D867	Exhibit X9, Guttman, E. et al., IETF RFC 2504, "Users' Security Handbook" (February 1999) Is Accessible At: http://www.ietf.org/rfc/rfc2504.txt	
	D868	Exhibit Y3, Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989 ("RFC1123").	
	D869	Exhibit Y4, Atkinson, R., RFC 1825, "Security Architecture for the Internet Protocol (August 1995) Is Accessible At: http://www.ietf.org/rfc/rfc1825.txt	
	D870	Exhibit Y5, Housley, R. et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (January 1999) Is accessible At: http://www.ietf.org/rfc/rfc2459.txt	
	D871	Exhibit A, U.S. Patent 7,418,504	
	D872	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,418,504)	
	D873	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D874	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in view of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D875	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D876	Exhibit C4, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D877	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed, and Beser	
	D878	Exhibit C6, Claim Chart – USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D879	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D880	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D881	Exhibit D1, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act. 6:2010cv00417 (E.D. Tex)	
	D882	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. against Apple Inc. Based on the 7,418,504	
	D883	Exhibit X5, Eastlake, D., et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)" (March 1999)	
	D884	Exhibit X6, Kent, S. IETF RFC 2401, "Security Architecture for the Internet Protocol, (November1998) http://www.ietf.org/rfc/rfc2401.txt	
	D885	Exhibit X8, Postel, J. et al., IETF RFC 920, "Domain Requirements" (October 1984) Is Accessible at http://www.ietf.org/rfc/rfc920.txt	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	41	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D886	Exhibit X10, Reed, M. et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996.	
	D887	Request for Inter Partes Reexamination Transmittal form	
	D888	Transmittal Letter	
	D889	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D890	Exhibit D-7, "Thomas": Brian Thomas, "Recipe for E-Commerce, IEEE Internet Computing, (Nov.-Dec. 1997)	
	D891	Exhibit D-9, "Kent II": Stephen Kent & Randall Atkinson, "IP Encapsulating Security Payload (ESP)," Internet Engineering Task Force, Internet Draft (Feb. 1998)	
	D892	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser (Came from Inval. Cisco dtd 11/18/11)	
	D893	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D894	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D895	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D896	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D897	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D898	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D899	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D900	211 Request for Inter Partes Reexamination	
	D901	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D902	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D903	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D904	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D905	Exhibit C6, USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D906	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D907	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D908	504 Request for Inter Partes Reexamination	
	D909	Defendants' Supplemental Joint Invalidity Contentions	
	D910	Exhibit 226, Securing Web Access with DCE vs. Claims of the '135 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	42	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D911	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D918	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D921	Exhibit 237, U.S. '648 vs. Claims of the '135 Patent	
	D922	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D923	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D924	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D925	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D926	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D927	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D928	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D929	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D930	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D931	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D932	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D933	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D934	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D936	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D937	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D938	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	D939	Exhibit A, Aventail Press Release, May 2, 1997	
	D940	Exhibit B, InfoWorld, "Aventail Delivers Highly Secure, Flexible VPN Solution," InfoWorld, page 64D, (1997)	
	D941	Exhibit C, Aventail AutoSOCKS v2.1 Administrator's Guide	
	D942	Exhibit D, Aventail Press Release, October 12, 1998	
	D943	Exhibit G, Aventail Press Release, May 26, 1999	
	D944	Exhibit H, Aventail Press Release, August 9, 1999	
	D945	Exhibit J, "Aventail ExtraNet Center 3.1: Security with Solid Management, Network Computing, June 28, 1999	
	D946	Petition in Opposition to Patent Owner's Petition to Vacate Inter Partes ReExamination Determination on Certain Prior Art	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Dennis G. Bonshock
Sheet	43	of	52	Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D947	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D948	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under U.S.C. § 311	
	D949	Exhibit C1, Claim Chart Aventail Connect v3.1	
	D950	Exhibit C2, Claim Chart Aventail Connect v3.01	
	D951	Exhibit C3, Claim Chart Aventail AutoSOCKS	
	D952	Exhibit C4, Claim Chart Wang	
	D953	Exhibit C5, Claim Chart Beser	
	D954	Exhibit C6, Claim Chart BINGO	
	D955	Exhibit X6, U.S. Patent 6,496,867	
	D956	Exhibit X10, U.S. Patent 4,885,778	
	D957	Exhibit X11, U.S. Patent 6,615,357	
	D958	Exhibit Y3, U.S. Patent 5,950,519	
	D959	Request for Inter Partes Reexamination Transmittal Form	
	D960	Transmittal Letter	
	D961	Exhibit D, v3.1 Administrator's Guide	
	D962	Exhibit E-1, Claim Charts Applying Kiuchi to Various Claims of the '135 Patent	
	D963	Exhibit E-2, Claim Charts Applying Wesinger to Various Claims of the '135 Patent	
	D964	Exhibit E-3, Claim Charts Applying Solana to Various Claims of the '135 Patent	
	D965	Exhibit E-4, Claim Charts Applying Aziz to Various Claims of the '135 Patent	
	D966	Request for Inter Partes Reexamination Transmittal Form	
	D967	Request for Inter Partes Reexamination	
	D968	PTO Form 1449	
	D969	Exhibit C1, Claim Chart Aventail Connect v3.01	
	D970	Exhibit C2, Claim Chart Aventail AutoSOCKS	
	D971	Exhibit C3, Claim Chart BINGO	
	D972	Exhibit C4, Claim Chart Beser	
	D973	Exhibit C5, Claim Chart Wang	
	D974	Transmittal Letter	
	D975	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D976	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D977	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D978	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D979	Exhibit E-3, Claim Charts Applying Blum to Claims of the '151 Patent	
	D980	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D981	Exhibit E-5, Claim Charts Applying Kiuchi and Edwards, and Kiuchi, Edwards, and Martin to Claims of the '151 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	44	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D982	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D983	Exhibit A, U.S. Patent 6,839,759	
	D984	Exhibit C-1, U.S. Patent 6,502,135	
	D985	Exhibit E-1, Claim Charts Applying Kiuchi, as Primary Reference to the '759 Patent	
	D986	Exhibit E-2, Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D987	Exhibit E-3, Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D988	Exhibit E-4, Claim Charts Applying Kent in View of Caronni as a Primary Combination of References to the '759 Patent	
	D989	Request for Inter Partes Reexamination Transmittal Form	
	D990	Request for Inter Partes Reexamination	
	D991	PTO Form 1449	
	D992	Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D993	Request for Inter Partes Reexamination	
	D994	Request for Inter Partes Reexamination Transmittal Form	
	D995	Request for Inter Partes Reexamination	
	D996	Request for Inter Partes Reexamination Transmittal Form	
	D997	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D998	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D999	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D1000	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D1001	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D1002	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D1003	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1004	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1005	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D1006	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D1007	Exhibit B1, File History of U.S. Patent 7,418,504	
	D1008	Exhibit B2, File History of U.S. Patent Application No. 09/558,210	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	45	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1009	Exhibit D-10, Gaspoz et al., “VPN on DCE: From Reference Configuration to Implementation,” Bringing Telecommunication Services to the People – IS&N ’95, Third International Conference on Intelligence in Broadband Services and Networks, October 1995 Proceedings, Lecture Notes in Computer Science, Vol. 998 (Springer, 1995)	
	D1010	Exhibit D-11, Copy of U.S. Patent No. 6,269,099	
	D1011	Exhibit D-11, Copy of U.S. Patent No. 6,560,634	
	D1012	Exhibit D-13, Pallen, “The World Wide Web,” British Medical Journal, Vol. 311 at 1554 (Dec. 1995)	
	D1013	Exhibit D-14, Rivest et al., “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, 21:120-126 (Feb. 1978)	
	D1014	Exhibit D-15, Copy of U.S. Patent No. 4,952,930	
	D1015	Exhibit D-17, Pfaffenberger, Netscape Navigator 3.0: Surfing the Web and Exploring the Internet, Academic Press (1996)	
	D1016	Exhibit D-18, Gittler et al., “The DCE Security Service,” Hewlett-Packard Journal, pages 41-48 (Dec. 1995)	
	D1017	Exhibit D-6, Copy of U.S. Patent No. 5,689,641	
	D1018	Exhibit D-9, Lawton, “New Top-Level Domains Promise Descriptive Names,” Sunworld Online, 1996	
	D1019	Exhibit E-1, Copy of Catalog Listing by IBM for RS/6000 Redbooks Collection which includes a Link to the *Lendenmann* reference. The link to the *Lendenmann* reference was archived at archive.org on December 7, 1998 and retrieved by the Wayback Machine	
	D1020	Exhibit E-10, copy of an Archived Version of the Lawton reference archived at archive.org on February 19, 1999 and retrieved by the Wayback Machine	
	D1021	Exhibit E-11, Abstracts of the Proceedings of the Symposium on Network and Distributed System Security, 1996, Archived at archive.org on April 10, 1997, and retrieved by the Wayback Machine	
	D1022	Exhibit E-12, 1996 Symposium on Network and Distributed System Security, Website Archived by archive.org (Apr. 10, 1997), Retrieved by the Wayback Machine at http://web.archive.org/web/19970410114853/http://computer.org/cspress/catalog/proc9.htm.	
	D1023	Exhibit E-13, Copy of Search Results for ISBN 0-12-553153-2 (Pfaffenberger) from www.isbnsearch.org	
	D1024	Exhibit F-1, Claim Charts applying Lendenmann as a Primary Reference to the ’504 Patent.	
	D1025	Exhibit F-2, Claim Charts applying Aziz as a Primary Reference to the ’504 Patent	
	D1026	Exhibit F-3, Claim Charts applying Kiuchi and Pfaffenberger as Primary References to the ’504 Patent	
	D1027	Exhibit E-2, First Page of U.S. Patent No. 5,913,217 published June 15, 1999 and citing a portion of the Lendenmann reference as a prior art reference	
	D1028	Exhibit E-3, Request for Comments 2026, “The Internet Standards Process – Revision 3,” October 1996	
	D1029	Exhibit E-4, First Page of U.S. 5,463,735, published October 31, 1995 and citing RFC 793 as a prior art Reference	
	D1030	Exhibit E-5, Copy of catalog listing from Boston University Digital Common Website, listing the Martin reference with an issue date of February 21, 1998	
	D1031	Exhibit E-6, Copy of Technical Reports Archive Listing from Boston University Computer Science Department which includes a link to the Martin paper. The link to the Martin paper was archived at archive.org on January 22, 1998 and Retrieved by the Wayback Machine	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	46	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1032	Exhibit E-7, Boston University Computer Science Department Technical Reports Instructions, available at: http://www.cs.bu.edu/techreports/INSTRUCTIONS	
	D1033	Exhibit E-8, U. Möller, "Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe," Diplomarbeit, Universität Hamburg (July 16, 1999), citing to Martin at page 77.	
	D1034	Exhibit E-9, First page of U.S. 5,737,423, published April 7, 1998 and citing Schneier as Prior Art Reference	
	D1035	Request for Inter Partes ReExamination; U.S. Patent 7,418,504	
	D1036	Request for Inter Partes ReExamination Transmittal Form; U.S. Patent 7,418,504	
	D1037	PTO Form 1449	
	D1038	Exhibit C1, Claim Chart – USP 7,921,211 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1039	Exhibit C2, Claim Chart – USP 7,921,211 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1040	Exhibit C3, Claim Chart – USP 7,921,211 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1041	Exhibit C4, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2230 and further in conjunction with RFC 920, Reed and Beser	
	D1042	Exhibit C5, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1043	Exhibit C6, Claim Chart – USP 7,921,211relative to Beser, Alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1044	Exhibit C7, Claim Chart – USP 7,921,211 relative to RFC 2230, alone and in conjunction with RFC 2401, Reed, and Beser	
	D1045	Exhibit C8, Claim Chart – USP 7,921,211 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1046	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1047	Exhibit C1, Claim Chart – USP 7,418,504 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1048	Exhibit C2, Claim Chart – USP 7,418,504 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1049	Exhibit C3, Claim Chart – USP 7,418,504 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1050	Exhibit C5, Claim Chart – USP 7,418,504 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1051	Exhibit C6, USP 7,418,504 relative to Beser, alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1052	Exhibit C7, Claim Chart – USP 7,418,504 relative to RFC 2230, alone and in conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1053	Exhibit C8, Claim Chart – USP 7,418,504 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1054	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1055	Exhibit 226, Securing Web Access with DCE vs. Claims of the '135 Patent	
	D1056	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Dennis G. Bonshock
Sheet	47	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D1063	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D1064	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D1065	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D1066	Exhibit 237, U.S. '072 vs. Claims of the '135 Patent	
	D1067	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D1068	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D1069	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D1070	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D1071	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D1072	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D1073	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D1074	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D1075	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D1076	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D1077	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D1078	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D1079	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D1081	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D1083	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	D1084	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1087	Exhibit B1, File History of U.S. Patent 7,921,211	
	D1088	Exhibit B2, File History of U.S. Patent Application No. 10/714,849	
	D1089	Exhibit B4, *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009)	
	D1090	Exhibit D15, U.S. Patent 4,952,930	
	D1091	Exhibit F1, Claim Charts Applying Lendenmann as a Primary Reference to the '211 Patent	
	D1092	Exhibit F2, Claim Charts Applying Aziz as a Primary Reference to the '211 Patent	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Control Number	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Dennis G. Bonshock
Sheet	48	of	52	Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1093	Exhibit F3, Claim Charts Applying Kiuchi and Pfaffenberger as Primary References to the '211 Patent	
	D1094	Exhibit 2, Letter and attachment from Ramzi Khazen, Counsel for VirnetX, to Dmitriy Kheyfits, Counsel for Cisco Systems (June 23, 2011)	
	D1095	Exhibit P, Malkin, "Dial-In Virtual Private Networks Using Layer 3 Tunneling"	
	D1096	Exhibit Q, Ortiz, "Virtual Private Networks: Leveraging the Internet"	
	D1097	Exhibit R, Keromytix, "Creating Efficient Fail-Stop Cryptographic Protocols"	
	D1098	Transcript of Markman Hearing Dated January 5, 2012	
	D1099	Declaration of John P. J. Kelly, Ph.D	
	D1100	Defendants' Responsive Claim Construction Brief; Exhibits A–P and 1-7	
	D1101	Joint Claim Construction and Prehearing Statement Dated 11/08/11	
	D1102	Exhibit A: Agreed Upon Terms Dated 11/08/11	
	D1103	Exhibit B: Disputed Claim Terms Dated 11/08/11	
	D1104	Exhibit C: VirnetX's Proposed Construction of Claim Terms and Supporting Evidence Dated 11/08/11	
	D1105	Exhibit D: Defendant's Intrinsic and Extrinsic Support Dated 11/08/11	
	D1106	Declaration of Austin Curry in Support of VirnetX Inc.'s Opening Claim Construction Brief	
	D1107	Declaration of Mark T. Jones Opening Claims Construction Brief	
	D1108	VirnetX Opening Claim Construction Brief	
	D1109	VirnetX Reply Claim Construction Brief	
	D1110	European Search Report from corresponding EP Application Number 11005789 (Our Ref.: 077580-0142)	
	D1111	European Search Report from corresponding EP Application Number 11005792 (Our Ref.: 077580-0143)	
	D1112	ITU-T Recommendation H.323, "Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System," International Telecommunications Union, pages 1-128, February 1998	
	D1113	ITU-T Recommendation H.225.0, "Infrastructure of Audiovisual Services – Transmission Multiplexing and Synchronization. Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication systems," International Telecommunication Union, pages 1-155, February 1998	
	D1114	ITU-T Recommendation H.235, "Infrastructure of Audiovisual Services – Systems Aspects. Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals," International Telecommunication Union, pages 1-39, February 1998	
	D1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	D1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	D1117	Transmittal Letters (Patent No.8,051,181)	
	D1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	
	D1119	Transcript of Hopen Deposition dated April 11, 2012 (57 pages)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,949
				Filing Date	March 28, 2012
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Dennis G. Bonshock
Sheet	49	of	52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1120	Claim Construction Memorandum Opinion and Order in Case No. 6:10-CV-417 (31 pages)	
	D1121	Declaration of Angelos D. Keromytic, Ph.D. in Control No. 95/001,682 (98 pages)	
	D1122	Declaration of Dr. Robert Dunham Short III in Control Nos. 95/001,679; 95/001,682 (6 pages)	
	D1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.) (2 pages)	
	D1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. in Control No. 95/001,269 (9 pages)	
	D1125	Exhibit A-4, Redacted Deposition of Chris Hopen from VirnetX, Inc. v. Cisco Systems, Inc., No. 6:07-CV 417 (E.D. Tex. April 11, 2012 (5 pages)	
	D1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999 (23 pages)	
	D1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects (95 pages)	
	D1128	Exhibit B-3, Maryann Lawlor, Transient Partnerships Stretch Security Policy Management, Signal Magazine (Sept. 2001) http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes (5 pages)	
	D1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html. (5 pages)	
	D1130	Time Greene, CEO's Chew the VPN Fat, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch (6 pages)	
	D1131	Peter Alexander Invalidity Report in Case No. 6:10-cv-000417 (220 pages)	
	D1132	Defendants' Second Supplemental Joint Invalidity Contentions in Case No. 6:10-cv-0417 (3 pages)	
	D1133	Exhibit 118A, Altiga VPN System vs. Claims of the '135 Patent (251 pages)	
	D1134	Exhibit 119A, Altiga VPN System vs. Claims of the '151 Patent (73 pages)	
	D1135	Exhibit 120A, Altiga VPN System vs. Claims of the '180 Patent (78 pages)	
	D1136	Exhibit 121A, Altiga VPN System vs. Claims of the '211 Patent (95 pages)	
	D1137	Exhibit 122A, Altiga VPN System vs. Claims of the '504 Patent (95 pages)	
	D1138	Exhibit 123A, Altiga VPN System vs. Claims of the '759 Patent (123 pages)	
	D1139	Exhibit 12A, SSL 3.0 vs. Claims of the '135 Patent (25 pages)	
	D1140	Exhibit 13A, SSL 3.0 vs. Claims of the '504 Patent (33 pages)	
	D1141	Exhibit 14A, SSL 3.0 vs. Claims of the '211 Patent (33 pages)	
	D1142	Exhibit 228A, Understanding OSF DCE 1. for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '135 Patent (21 pages)	
	D1143	Exhibit 229A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '151 Patent (15 pages)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO			
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		*Complete if Known*	
(Use as many sheets as necessary)		*Control Number*	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 50 of 52		*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1144	Exhibit 230A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '180 Patent (25 pages)	
	D1145	Exhibit 231A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '211 Patent[2]	
	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '504 Patent (44 pages)	
	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '759 Patent (28 pages)	
	D1148	Exhibit 255, Schulzrinne vs. Claims of the '135 Patent (28 pages)	
	D1149	Exhibit 256, Schulzrinne vs. Claims of the '504 Patent (122 pages)	
	D1150	Exhibit 257, Schulzrinne vs. Claims of the '211 Patent (122 pages)	
	D1151	Exhibit 258, Schulzrinne vs. Claims of the '151 Patent (49 pages)	
	D1152	Exhibit 259, Schulzrinne vs. Claims of the '180 Patent (41 pages)	
	D1153	Exhibit 260, Schulzrinne vs. Claims of the '759 Patent (74 Pages)	
	D1154	Exhibit 261, SSL 3.0 vs. Claims of the '151 Patent (14 pages)	
	D1155	Exhibit 262, SSL 3.0 vs. Claims of the '759 Patent (24 pages)	
	D1156	Exhibit 263, Wang vs. Claims of the '135 Patent (59 pages)	
	D1157	Wang vs. Claims of the '504 Patent (55 pages)	
	D1158	Wang vs. Claims of the '211 Patent (56 pages)	
	D1159	Exhibit 1, Alexander CV (22 pages)	
	D1160	Exhibit 2, Materials Considered by Peter Alexander (16 pages)	
	D1161	Exhibit 3, Cross Reference Chart (24 pages)	
	D1162	Exhibit 4, RFC 2543 vs. Claims of the '135 Patent (43 pages)	
	D1163	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent (46 pages)	
	D1164	Exhibit 6, RFC 2543 vs. Claims of the '211 Patent (46 pages)	
	D1165	Exhibit 7, The Schulzrinne Presentation vs. Claims of the '135 Patent (32 pages)	
	D1166	Exhibit 8, The Schulzrinne Presentation vs. Claims of the '504 Patent (36 pages)	
	D1167	Exhibit 9, The Schulzrinne Presentation vs. Claims of the '211 Patent (36 pages)	
	D1168	Exhibit 10, The Schulzrinne Presentation vs. Claims of the '151 Patent (15 pages)	
	D1169	Exhibit 11, The Schulzrinne Presentation vs. Claims of the '180 Patent (11 pages)	
	D1170	Exhibit 12, The Schulzrinne Presentation vs. Claims of the '759 Patent (29 pages)	
	D1171	Exhibit 13, SSL 3.0 vs. Claims of the '135 Patent (33 pages)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	51	of	52

Complete if Known	
Control Number	95/001,949
Filing Date	March 28, 2012
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Dennis G. Bonshock
Attorney Docket Number	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1172	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent (38 pages)	
	D1173	Exhibit 15, SSL 3.0 vs. Claims of the '211 Patent (39 pages)	
	D1174	Exhibit 16, SSL 3.0 vs. Claims of the '151 Patent (10 pages)	
	D1175	Exhibit 17, SSL 3.0 vs. Claims of the '759 Patent (25 pages)	
	D1176	Exhibit 18, Kiuchi vs. Claims of the '135 Patent (30 pages)	
	D1177	Exhibit 19, Kiuchi vs. Claims of the '504 Patent (35 pages)	
	D1178	Exhibit 20, Kiuchi vs. Claims of the '211 Patent (35 pages)	
	D1179	Exhibit 21, Kiuchi vs. Claims of the '151 Patent (8 pages)	
	D1180	Exhibit 22, Kiuchi vs. Claims of the '180 Patent (19 pages)	
	D1181	Exhibit 23, Kiuchi vs. Claims of the '759 Patent (25 pages)	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401 vs. Claims of the '135 Patent (51 pages)	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '504 Patent (45 pages)	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '211 Patent (45 pages)	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '151 Patent (18 pages)	
	D1186	Exhibit 28 (2 pages)	
	D1187	Exhibit 29, The Altiga System vs. Claims of the '135 Patent (35 pages)	
	D1188	Exhibit 30, The Altiga System vs. Claims of the '504 Patent (40 pages)	
	D1189	Exhibit 31, The Altiga System vs. Claims of the '211 Patent (41 pages)	
	D1190	Exhibit 32, The Altiga System vs. Claims of the '759 Patent (35 pages)	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '135 Patent (64 pages)	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '504 Patent (39 pages)	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '211 Patent (41 pages)	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '151 Patent (19 pages)	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '180 Patent (33 pages)	
	D1196	Exhibit 38, Kent vs. Claims of the '759 Patent (17 pages)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

IDS Form PTO/SB/08: Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*		***Complete if Known***	
		Control Number	95/001,949
		Filing Date	March 28, 2012
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Dennis G. Bonshock
Sheet 52	of 52	*Attorney Docket Number*	077580-0160

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent (48 pages)	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent (48 pages)	
	D1199	Exhibit 41, Aziz ('646) vs. Claims of the '759 Patent (24 pages)	
	D1200	Exhibit 42, The PIX Firewall vs. Claims of the '759 Patent (24 pages)	
	D1201	Exhibit A-1, Kiuchi vs. Claims of the '135 Patent (181 pages)	
	D1202	Exhibit B-1, Kiuchi vs. Claims of the '211 Patent (200 pages)	
	D1203	Exhibit C-1, Kiuchi vs. Claims of the '504 Patent (278 pages)	
	D1204	Exhibit D, Materials Considered (3 pages)	
	D1205	Exhibit E, CV of Stuart G. Stubblebine, Ph.D (19 pages)	
	D1206	Exhibit F, Claim Construction Chart (7 pages)	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents (60 pages)	
	D1208	Cisco Comments and Petition for Reexamination in Control No. 95/001,679 dated June 14, 2012 (69 pages)	
	D1209	Exhibit S, Declaration of Nathaniel Polish, Ph.D in Control No. 95/001,679 (5 pages)	
	D1210	Exhibit R, Excerpts from Patent Owner & Plaintiff VimetX Inc. 's First Amended P.R. 3-1 and 3-2 Disclosure of Asserted Claims and Infringement Contentions (53 pages)	
	D1211	Third Party Requester Comments dated June 25, 2012 - After Non Final Office Action in Control No. 95/001,788 (37 pages)	
	D1212	Reexam Affidavit/Declaration/Exhibit Filed by 3rd Party on June 25, 2012 in Control No. 95/001,788 (19 pages)	
	D1213	Extended European Search Report dated 03/26/12 from Corresponding European Application Number 11005793.2 (077580-0144) (6 pages)	
	D1214	Bergadano, et al., "Secure WWW Transactions Using Standard HTTP and Java Applets," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998 (12 pages)	
	D1215	Alexander Invalidity Expert Report dated May 22, 2012 with Exhibits (1542 pages)	
	D1216	Transcript of Deposition of Peter Alexander dated July 27, 2012 (55 pages)	
	D1217	Cisco '151 Comments by Third Party Requester dated August 17, 2012 with Exhibits (211 pages)	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dated August 17, 2012 (4 pages)	
	D1219	Transcript of August 22, 2012 Deposition of Stuart Stubblebine (69 pages)	

Examiner Signature	/Dennis Bonshock/	Date Considered	01/03/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.B./

Reexamination	Application/Control No. 95001949	Applicant(s)/Patent Under Reexamination 8051181
	Certificate Date	Certificate Number

Requester Correspondence Address: □ **Patent Owner** ☒ **Third Party**

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

LITIGATION REVIEW ☒	DGB (examiner initials)	05/23/2012 (date)

Case Name	Director Initials
VirnetX Inc. v. Cisco Systems, Inc., Apple, Inc., et al., Civ	/AJK/ for IY

COPENDING OFFICE PROCEEDINGS

TYPE OF PROCEEDING	NUMBER

Search Notes	**Application/Control No.** 95001949	**Applicant(s)/Patent Under Reexamination** 8051181
	Examiner DENNIS BONSHOCK	**Art Unit** 3992

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
Reviewed all prosecution history	5-22-12	dgb
Reviewed all prosecution history	1-3-13	dgb

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U.S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE
COMMUNICATION LINK BETWEEN
COMPUTERS OF VIRTUAL PRIVATE
NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No.: 4522

VIA EFS WEB

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S PETITION FOR EXTENSION OF TIME PURSUANT TO 37 C.F.R. § 1.956

VirnetX Inc., the owner of the above-referenced patent, hereby petitions for a one-month extension of time for responding to the Office Action mailed January 16, 2013 ("Office Action"), in the above-identified reexamination proceeding. A response to the Office Action is currently due on February 16, 2013.

Pursuant to 37 C.F.R. § 1.956, this petition for an extension of time (1) is being filed well before the due date for the response, and (2) sets forth sufficient reasons for the extension, as detailed below. VirnetX is concurrently submitting payment of the requisite fee. If any additional fees are due, please charge them to Deposit Account 06-0916.

VirnetX's counsel has begun preparing a response to the Office Action. VirnetX, however, seeks an extension of time of one month to allow VirnetX additional time to prepare and file a suitable response.

The nature and complexity of the Office Action warrant an extension of time of one month. The Office Action itself is 110 pages in length, and it addresses 11 grounds of rejection based on 12 different references. In doing so, the Office Action addresses positions in the 319-page Request for Reexamination and other filings in this proceeding. Accordingly, analyzing the Office Action and preparing a complete response will require substantial time and effort.

Additionally, a complete response to the Office Action may require an accompanying declaration from VirnetX's expert. VirnetX is working with its expert and investigating the need for such a declaration. Coordinating with the expert and preparing a declaration may take additional time.

Finally, VirnetX is concurrently involved in several other pending reexamination proceedings—namely, control nos. 95/001,679 and 95/001,682 involving U.S. Patent No. 6,502,135; control nos. 95/001,697 and 95/001,714 involving U.S. Patent No. 7,490,151; control no. 95/001,746 involving U.S. Patent No. 6,839,759; control nos. 95/001,788 and 95/001,851 involving U.S. Patent No. 7,418,504; control nos. 95/001,789 and 95/001,856 involving U.S. Patent No. 7,921,211; and control no. 95/001,792 involving U.S. Patent No. 7,188,180. These proceedings will demand attention from VirnetX and strain its resources during the period for response to the Office Action. Tending to these other proceedings while preparing a response to the instant Office Action will require additional time and effort.

In view of the foregoing, VirnetX requests an extension of time of one month to complete the response to the Office Action currently due on February 16, 2013.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 22, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
Victor Larson et al.	)	Control No.: 95/001,949
U.S. Patent No. 8,051,181	)	Group Art Unit: 3992
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Petition for Extension of Time Pursuant to 37 C.F.R. § 1.956 was served by first-class mail on January 22, 2013, on counsel for the third party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 22, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Joseph Edwin Palys./Sheryl Lewis
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**200**

Electronic Acknowledgement Receipt

EFS ID:	14753616
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	22-JAN-2013
Filing Date:	28-MAR-2012
Time Stamp:	12:11:17
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$200
RAM confirmation Number	16070
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		PEOT.pdf	138740 2e34aab6f765ec0be3f37c7aecd12ad8280c38d2	yes	3
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Reexam Request for Extension of Time		1	2	
	Reexam Certificate of Service		3	3	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30425 4cdf0dc6f01c5f122bfaa0f7008492420eeafa3a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	169165		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 01/24/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	PAPER NUMBER
3992	
MAIL DATE	DELIVERY MODE
01/24/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS

Date:

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Decision on Petition for Extension of Time in Reexamination	Control No.:95/001,949

1. THIS IS A DECISION ON THE PETITION FILED 1/22/13

2. THIS DECISION IS ISSUED PURSUANT TO:
A. □ 37 CFR 1.550(c) – The time for taking any action by a patent owner in an *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
B. ☒ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS
Patent owner requests that the period for responding to the Office action mailed on 1/16/13, which sets a one(1) month period for filing a response thereto, be extended by one(1) month.

A. ☒ Petition fee per 37 CFR §1.17(g)):
i. □ Petition includes authorization to debit a deposit account.
ii. □ Petition includes authorization to charge a credit card account.
iii. □ Other: ______________.
B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
C. ☒ Petition was timely filed.
D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
A. ☒ Granted or □ Granted-in-part for ______________, because petitioner provided a factual accounting that established sufficient cause. (See 37 CFR 1.550(c) and 37 CFR 1.956).
□ Other/comment: ____.
B. □ Dismissed because:
i. □ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).
ii. □ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
iii. □ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
iv. □ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
v. □ The petition is moot.
vi. □ Other/comment:

5. CONCLUSION

Telephone inquiries with regard to this decision should be directed to Alexander Kosowski at 571-272-3744. In his/her absence, calls may be directed to Mark Reinhart at 571-272-1611 or Sudhanshu C. Pathak at 571-272-5509 in the Central Reexamination Unit.

/Alexander Kosowski/ SPE, CRU 3992
[*Signature*] (Title)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 03/13/2013

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	**PAPER NUMBER**
3992	
MAIL DATE	**DELIVERY MODE**
03/13/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

FINNEGAN, HENDERSON, FARABOW,
GARRET & DUNNER LLP
901 New York Avenue, N.W.
Washington, D.C. 20001-4413

(For Patent Owner)

SIDLEY AUSTIN LLP
717 North Harwood
Suite 3400
Dallas, Texas 75201

(For Petitioner)

Inter Partes Reexamination Proceeding
Control No.: 95/001,949
Filed: March 28, 2012
For: U.S. Patent No. 8,051,181

: **DECISION**
: **DISMISSING**
: **PETITION**
: **TO ALIGN SCHEDULES**

This is a decision on third party requester's "Petition Under 37 CFR § 1.182 To Align Schedules of Related Proceedings" ("petition under 1.182"), filed on December 5, 2012, and on "Patent Owner's Petition In Opposition To Third-Party Requester Apple Inc.'s Petition To Align Schedules" ("the opposition"), filed on December 13, 2012.

The petition under 37 CFR 1.182 and the opposition are before the Office of Patent Legal Administration.

The petition under 37 CFR 1.182 is dismissed for the reasons set forth herein.

Note that all citations to 35 U.S.C. Chapter 31 are to the statute in effect as of the filing date of the *inter partes* reexamination proceeding.

BACKGROUND

1. On August 11, 2010, VirnetX Inc. ("patent owner") asserted U.S. Patent Nos. 6,502,135 (the '135 patent"), 7,490,151 ("the '151 patent"), 6,839,759 ("the 759 patent"), 7,188,180 ("the '180 patent"), and 7,418,504 ("the '504 patent") in the Eastern District of Texas (*VirnetX Inc. v. Cisco Sys., Inc., et al.*, No. 6:10-cv-00417). Apple Inc. ("Apple") is

included as one of the named defendants. Patent owner additionally asserted U.S. Patent No. 7,921,211 ("the '211 patent") in an Amended Complaint filed on April 5, 2011.

The '1788 reexamination proceeding:

2. On October 18, 2011, a request for *inter partes* reexamination of claims 1-60 of the '504 patent was filed by a third party requester, which request was assigned Reexamination Control No. 95/001,788 ("the '1788 proceeding"). The request identified Apple as the real party in interest. On December 29, 2011, the Office issued an order granting the request for *inter partes* reexamination.

3. On December 29, 2011, the Office issued an Office Action rejecting claims 1-60 of the '504 patent. On March 29, 2012, patent owner responded to the Office Action. On June 25, 2012, Apple filed comments on the patent owner's response. On September 26, 2012, the Office issued an Action Closing Prosecution (ACP).

The '1789 reexamination proceeding:

4. On October 18, 2011, a request for *inter partes* reexamination of claims 1-60 of the '211 patent was filed by a third party requester, which request was assigned Reexamination Control No. 95/001,789 ("the '1789 proceeding"). The request identified Apple as the real party in interest. On January 18, 2012, the Office issued an order granting the request for *inter partes* reexamination in the '1789 proceeding.

5. On January 18, 2012, the Office issued an Office Action rejecting claims 1-60 of the '211 patent. On April 18, 2012, patent owner responded to the Office Action. On August 6, 2012, Apple filed comments on the patent owner's response. On September 26, 2012, the Office issued an ACP.

The '1949 reexamination proceeding:

6. On November 1, 2011, U.S. Patent No. 8,051,181 ("the '181 patent") issued to Larson et al. with 29 claims.

7. On March 28, 2012, a request for *inter partes* reexamination of claims 1-29 of the '181 patent was filed by a third party requester, which request was assigned Reexamination Control No. 95/001,949 ("the '1949 proceeding"). The request identified Apple as the real party in interest. On June 4, 2012, the Office issued an order granting the request for *inter partes* reexamination in the '1949 proceeding.

8. On June 4, 2012, the Office issued an Office Action rejecting claims 1-29 of the '181 patent. On September 4, 2012, patent owner responded to the Office Action. On October 22, 2012, Apple filed comments on the patent owner's response.

9. On December 5, 2012, Apple filed the instant petition paper entitled "Petition Under 37 CFR § 1.182 To Align Schedules Of Related Proceedings" ("the petition under 37 CFR 1.182").

10. On December 13, 2012, patent owner filed "Patent Owner's Petition In Opposition To Third-Party Requester Apple Inc.'s Petition To Align Schedules" ("the opposition").

11. On January 16, 2013, the Office mailed an ACP ("the January 16, 2013 ACP") in the '1949 proceeding.

Related proceedings:

12. Also, on December 5, 2012, Apple filed petition papers entitled "Petition Under 37 CFR § 1.182 To Align Schedules Of Related Proceedings" in Reexamination Control Nos. 95/001,697 and 95/001,682.

DECISION

Relevant Statutes, Regulations and Practice

35 U.S.C. § 314 provides, in part:

> (a) IN GENERAL.— Except as otherwise provided in this section, reexamination shall be conducted according to the procedures established for initial examination under the provisions of sections 132 and 133. In any *inter partes* reexamination proceeding under this chapter, the patent owner shall be permitted to propose any amendment to the patent and a new claim or claims, except that no proposed amended or new claim enlarging the scope of the claims of the patent shall be permitted.
>
> ****
>
> (c) SPECIAL DISPATCH.— Unless otherwise provided by the Director for good cause, all *inter partes* reexamination proceedings under this section, including any appeal to the Board of Patent Appeals and Interferences, shall be conducted with special dispatch within the Office.

Apple's Petition under 37 CFR 1.182 and Patent Owner's Opposition

In the petition under 37 CFR 1.182, Apple ("petitioner") requests that "the Office take actions to accelerate, and to thereby better align, the schedules of Reexamination Control No. 95/001,949 with the schedules of 95/001,788 and 95/001,789."[1] Specifically, petitioner requests the Office "to act promptly in issuing an Action Closing Prosecution in the '949 proceeding,[2] and to limit the period granted in that proceeding for Patent Owner and/or Requestor to respond to the ACP

[1] Petition under 37 CFR 1.182 at page 1.

[2] Petitioner uses the last three digits of the control number of each proceeding to identify the proceeding.

to no more than one month, and to take such other steps that will expedite issuance of a final decision in each of the three pending reexamination proceedings."[3]

In support of its request, petitioner states that "doing so will help align the schedules of the '949 proceeding with those of the '788 and '789 proceedings, in which ACPs have issued with a previously extended deadline for response of December 26, 2012 for each proceeding."[4] Specifically, petitioner asserts that because the three proceedings are "closely related" and "present similar and related issues of patentability over the prior art", "[t]aking steps to better align the schedules of the three proceedings will serve the public interest by providing for an efficient and expeditious review of final decisions of the Office concerning the three related patents."[5] Further, it is the position of the petitioner that expediting the conclusion of the '1949 proceeding will also "enable appeals of the three patents to be considered concurrently with any appeal arising from concurrent litigation pending in the Eastern District of Texas or International Trade Commission."[6] Petitioner asserts that "[a]ccelerating the '1949 proceeding is also the only path consistent with the Office's mandate to conduct *inter partes* reexamination proceedings with special dispatch."[7] Finally, petitioner asserts that "[a]ccelerating the '949 proceeding also will not prejudice the interests of the Patent Owner."[8]

In opposition to requester's petition under 37 CFR 1.182, patent owner asserts that "these reexaminations are already being appropriately conducted by the Office with the 'special dispatch' sought by Apple."[9] Patent owner further asserts that "contrary to Apple's representations, accelerating the '1,682, '1,697, and '1,949 proceedings would substantially prejudice Patent Owner" and "would not provide the Patent Owner adequate time and opportunity to respond."[10]

Discussion

In view of the mailing of the January 16, 2013 ACP, petitioner's request that the Office issue an ACP in the '1949 proceeding and limit the response period set forth therein to no more than one month is rendered moot.[11]

Petitioner's request that the Office "take such other steps that will expedite issuance of a final decision in each of the three pending reexamination proceedings"[12] is not practicable as a matter of Office administration. The timing of Office actions issued in reexamination proceedings is a matter of Central Reexamination Unit (CRU) docket management and internal administration by the Office. Each reexamination proceeding is conducted on its own merits and decisions therein

[3] Petition under 37 CFR 1.182 at page 4.
[4] *Id.*
[5] *Id.*
[6] *Id.* at page 5.
[7] *Id.* at page 6.
[8] *Id.*
[9] Opposition at page 4.
[10] *Id.* at pages 5-6 (noting that patent owner "must also respond to filings from Apple and Cisco in a large number of other reexaminations.")
[11] The January 16, 2013 ACP sets a time period for response of 30 days or one month (whichever is longer) from the mailing date of the ACP.
[12] Petition under 37 CFR 1.182 at page 4.

are decided on a case-by-case basis. The fact that the subject matter of the three proceedings is related and may present similar and related issues of patentability does not justify requiring the examiners to expedite issuance of actions in all three proceedings[13] at the expense of delaying other proceedings on the examiners' dockets. To do so would put an undue burden on each examiner with respect to docket management and the coordination thereof with other examiners.[14] Moreover, even if the examiners were to attempt such coordination, many circumstances in reexamination proceedings which are beyond the examiners' control could disrupt such coordination (*e.g.*, a petition or an improper paper that is filed in one, but not all, of the aligned proceedings).

Additionally, delaying one or more proceedings in order to align with and expedite another proceeding does not promote the mandate of 35 U.S.C. § 314 that all *inter partes* reexamination proceedings be conducted with special dispatch in the Office. Thus, the Office cannot commit to issuing Office actions simultaneously across various proceedings that are docketed to different examiners and that are at different stages of prosecution. Examiners will mail Office actions in proceedings as they are completed, irrespective of when Office actions are ready to be mailed in other proceedings. In granting equitable relief pursuant to 37 CFR 1.182, the Office must balance the equities of granting such relief with respect to all parties to the reexamination proceedings, as well as any impact on the Office. In this instance, the relief requested could prejudice the patent owner and place unwarranted administrative burden on the Office. Accordingly, for at least the aforementioned reasons, **the petition under 1.182 is dismissed**.

CONCLUSION

1. Requester's December 5, 2012 petition under 37 CFR 1.182 is dismissed.

2. Any questions concerning this communication should be directed to Erin M. Harriman, Legal Advisor, at 571-272-7747 or to the undersigned at 571-272-7726.

Pinchus M. Laufer
Senior Legal Advisor
Office of Patent Legal Administration

March 11, 2013

[13] In fact, petitioner is requesting the alignment of ongoing *inter partes* reexamination proceedings of five different patents. See "Petition Under 37 CFR § 1.182 To Align Schedules of Related Proceedings," filed December 5, 2012, in both Reexamination Control No. 95/001,697 and Reexamination Control No. 95/001,682.

[14] The Office notes that the examiner of the '1949 proceeding is different from the examiner of the '1788 and '1789 proceedings. The '1788 and '1789 proceedings demonstrate that, under certain circumstances (*e.g.*, requests filed at the same time and assigned to the same examiner), some proceedings may progress in substantial alignment.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No. 4522
	)	
	)	**VIA EFS WEB**
	)	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S PETITION TO REOPEN PROSECUTION

Pursuant to 37 C.F.R. § 1.181 and M.P.E.P. § 2672, VirnetX Inc., the owner of the above-referenced patent, submits that the Action Closing Prosecution in the above-identified reexamination proceeding was premature, and hereby requests that the Director reopen prosecution.

To the extent that entry and consideration of this petition require suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. A petition fee of $1,930 required by 37 C.F.R. § 1.20(c)(6) is being submitted with this petition. If any additional fee is due in connection with the filing of this petition, please charge it to Deposit Account 06-0916.

I. Background

Third-party requester Apple Inc. ("Apple") filed a Request for Reexamination ("Request") on March 28, 2012. The Office granted the Request and issued a first Office Action ("OA") on June 4, 2012, which adopted eleven of Apple's thirteen proposed rejections. In support of the rejections, the first Office Action incorporated nearly the entirety of the Request. VirnetX filed a response ("Response") to the first Office Action on September 4, 2012. Apple filed third-party Comments

("Comments") to VirnetX's Response on October 22, 2012. The Office issued an Action Closing Prosecution ("ACP") on January 16, 2013, maintaining each of the eleven rejections from the first Office Action and including a "Response to Arguments" section with several new bases for its rejections.

II. Argument

VirnetX respectfully submits that the ACP was premature. The M.P.E.P. instructs that an ACP is improper if the issues have not been fully developed. M.P.E.P. § 2671.01 (citing 37 C.F.R. § 1.949). Here, the ACP introduces several new bases for its rejections, extending beyond the proposed rejections in the Request that were incorporated by reference into the first Office Action. For example, the ACP adopts many new positions that the Requester presented for the first time in its Comments on VirnetX's Response and that are inconsistent with positions taken in the first Office Action. Prosecution should therefore be reopened to give VirnetX a sufficient opportunity to respond to these newly adopted positions, examples of which are provided below.

A. The ACP Adopts a New Basis for the Rejections Based on *Mattaway*

The ACP adopts a new rejection related to *Mattaway*, completely changing its analysis of what allegedly constitutes the "receiving, at a network address corresponding to the secure name associated with the first device, *a message from a second device of the desire[] to securely communicate with the first device*," as recited in claim 1 and similarly recited in claims 24, 26, and 29 (emphasis added).

The first Office Action, adopting the Request, asserted that the <CONNECT REQ> message in *Mattaway* disclosed the recited "message . . . of the desire[] to securely communicate." (OA at 5, incorporating Req. at 68-94.) The Office and Requester cited to two different protocols in *Mattaway*, and for each protocol focused on the <CONNECT REQ> message as allegedly disclosing the recited "message . . . of the desire[] to securely communicate." (Req. at 70-71, citing *Mattaway* 18:41-45 and Fig. 16A disclosing processing a <CONNECT REQ> message in the alleged first protocol; Req.

at 71, citing *Mattaway* 8:25-44 disclosing processing a <CONNECT REQ> message in the alleged second protocol.)

In its Response to the first Office Action, VirnetX pointed out that *Mattaway*'s <CONNECT REQ> message could not be the recited "message . . . of the desire[] to securely communicate" because it is not received at a network address corresponding to the secure name *associated with the alleged first device*, as required by claim 1. (Response at 21.)

The ACP, adopting new arguments presented for the first time in Apple's Comments on VirnetX's Response, now asserts that *Mattaway*'s <CALL> message corresponds to the recited "message . . . of the desire[] to securely communicate." (ACP at 34, "the process described in column 24, line 11 through 25, line 34, explains the callee receiving a request to communicate[] from the caller, to which the callee can either <REJECT>, or accept (<CALL ACK>) the call thereby establishing the connection.") *Mattaway* 24:11-25:34, as cited by the Office, deals exclusively with processing the <CALL> message sent between two webphones and has nothing to do with the <CONNECT REQ> message. Apple's Comments cite to the very same portions of *Mattaway* cited by the ACP, but neither the Request nor the first Office Action even mentioned these portions or anything about the <CALL> message when initially analyzing this claim recitation. (*Compare* Comments at 13-14, relying exclusively on the <CALL> message as allegedly disclosing the claimed feature *with* Req. at 70-71, failing to mention or cite to a portion of *Mattaway* describing the <CALL> message.)

Moreover, Fig. 17A of *Mattaway*, reproduced below, makes clear that the <CONNECT REQ> and <CALL> messages are distinct messages sent between different sets of devices at different times during the *Mattaway* call process.

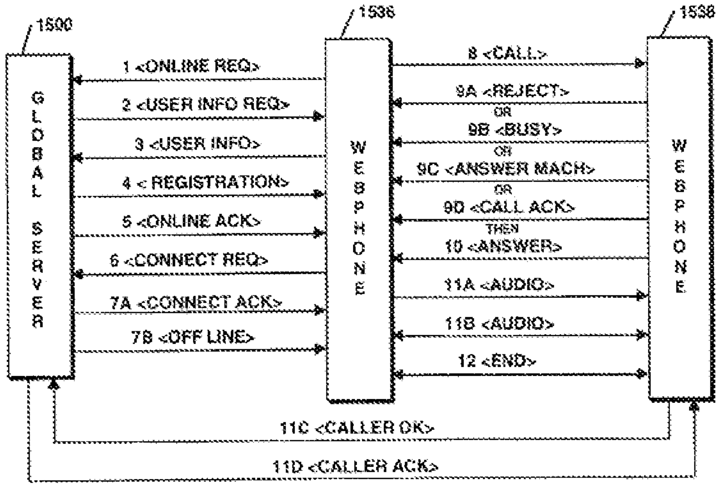


Figure 17A

It is improper for the Office to make such a drastic change in its anticipation analysis and then close prosecution, thereby limiting VirnetX's ability to respond to a brand new position. Prosecution should be reopened for at least this reason.

B. The ACP Adopts a New Basis for the Rejections Based on *Provino*

The ACP also adopts a new rejection related to *Provino*, shifting the focus from a domain name to an Internet address. The Request originally alleged that two different domain names in *Provino* are the claimed "secure name" and "unsecured name":

> *Provino* additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11.

(Req. at 168.) The Office adopted this portion of the Request in its first Office Action. (OA at 8, "This rejection was proposed by the third party requester in the Request, and it is adopted with regard to claims 1-15, 18-23, 28, and 29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.")

In the ACP, however, the Examiner now alleges that the claimed "secure name" does not correspond to "the Domain name stored in the VPN Name Server 32," but instead corresponds to an integer Internet address:

> Provino further teaches use of a secure name where the device [may] only establish a secure communication link upon receipt of the secure name (the integer Internet address which is registered on the VPN name server (see column 9, line 56 through column 10, lines 7, column 9, lines 17-27, and column 13, [lines] 26-67).

(ACP at 71.) As with *Mattaway*, the Office has drastically changed its rejection and then attempted to close prosecution. Because the Office has issued what is effectively a new rejection regarding *Provino* in the ACP, prosecution should be reopened.

C. The ACP Adopts a New Basis for the Rejections Based on *Lendenmann*

The ACP additionally adopts a new rejection based on *Lendenmann* for the "sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device" feature of claim 2.

Lendenmann discloses three different distributed computing models: (1) the client/server model, (2) the remote procedure call ("RPC") model, and (3) the data sharing model. (*Lendenmann* 8-9.) The first Office Action relied on *Lendenmann*'s RPC model as disclosing the above-referenced feature of claim 2. (Req. at 112-13, citing *Lendenmann* 173-79; OA at 7, incorporating this section of the Request by reference.) In its Response to the first Office Action, VirnetX traversed the rejection by explaining that the RPC model of *Lendenmann* does not disclose "sending a message . . . requesting a network address associated with the secure name of the second device" because, among other things, the RPC model involves searching for servers on criteria other than server names. (Response at 37-39.)

In the ACP, the Office did not contest VirnetX's arguments with respect to the RPC model of *Lendenmann*. (ACP at 61.) Rather, the Office changed course and instead relied exclusively on page 21 of *Lendenmann* as disclosing that *Lendenmann*'s Cell Directory Server ("CDS"), when given an X.500 name, returns a network address. (*Id.*, citing *Lendenmann* 21.) Yet this section of *Lendenmann* expressly states that the CDS "follows the client/server model." (*Lendenmann* 29.) Thus, in the ACP, the Office for the first time relies on the client/server model of *Lendenmann* instead of the RPC model. Prosecution should be reopened so that the issues can be fully developed regarding the rejection newly based on a different embodiment of *Lendenmann*.

D. The ACP Adopts a New Basis for the Rejections Based on *Johnson*

As with *Mattaway*, *Provino*, and *Lendenmann*, the ACP similarly adopts a new rejection regarding *Johnson*. The ACP relies on the dynamic address of the secure mail server 16 in *Johnson* as allegedly disclosing the "unsecured name" of claims 1, 21, 26, and 27—an entirely different element than was relied upon in the first Office Action.

The first Office Action incorporated the *Johnson* portion of the Request in its entirety and alleged that a number of different items in *Johnson* satisfy the claimed "unsecured name." (OA at 12, incorporating Req. at 270-318; Req. at 273-274.) These items include the domain name of the secure name server 14 that is purportedly registered with a DHCP, the domain names of the secure name server 14 and secure mail server 16 that are purportedly registered in the public DNS system, and "client identifiers" of the secure name server 14 and secure mail server 16. (OA at 12; Req. at 273-274.) But the Office or Requester never alleged that the dynamic address of secure mail server 16 is the "unsecured name." Rather, the Office and Requester stated:

> Further, because the secure name server 14 requires a proper log protocol combination, *the dynamic address of the secure electronic mail server 16 is not easily obtained*. The security of the "secure name" is further shown "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16. *Johnson* at 8:4-9.

(Req. at 272, emphasis added.)

In the ACP, the Office directly contradicts its statements in the first Office Action and relies on the dynamic address of the secure mail server 16 as allegedly satisfying the "unsecured name":

> The Examiner agrees with the third party requestor, the user at the first device requests access to the secure mail server via a "name" (secure) then *when they are authenticated via the secure name server, they are provided with the "address" (unsecure)* corresponding the provided "name" (see 11:20-37).

(ACP at 96, emphasis added.) This constitutes a new rejection that is at odds with the Office's previous statements, leaving VirnetX with an insufficient opportunity to respond. Accordingly, prosecution should be reopened.

The M.P.E.P. instructs that the Office should be liberal in reopening prosecution where the equities of the situation render such action appropriate, because a patent owner cannot continue the proceeding by re-filing under 37 C.F.R. § 1.53(b) or § 1.53(d), or by filing a Request for Continued Examination under 37 C.F.R. § 1.114. *See* M.P.E.P. § 2673.01.

Here, justice requires reopening prosecution. Many bases for the rejections have just recently been clarified or asserted for the first time in the ACP, but since the second Office Action was issued as an ACP, the Office has severely compromised VirnetX's opportunity to fully address the new issues. Accordingly, the ACP was premature and prosecution should be reopened to fully develop the issues in this proceeding.

III. Conclusion

In view of the foregoing, VirnetX submits that the premature timing of the ACP compromises VirnetX's opportunity to fully address the issues raised in this proceeding, and respectfully requests that the Director reopen prosecution.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 18, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor Larson et al.) Control No.: 95/001,949
)
U. S. Patent No. 8,051,181) Group Art Unit: 3992
)
Issued: November 1, 2011) Examiner: Dennis G. Bonshock
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 4522
COMMUNICATION LINK BETWEEN)
COMPUTERS OF A VIRTUAL PRIVATE) **VIA EFS WEB**
NETWORK)

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Petition to Reopen Prosecution Pursuant to 37 C.F.R. § 1.181 was served by first-class mail on March 18, 2013, on counsel for the third party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 18, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Joseph Edwin Palys./Connie Sisk
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION IN REEXAM PROCEEDING	1824	1	1930	1930
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
	Total in USD ($)			**1930**

Electronic Acknowledgement Receipt

EFS ID:	15282808
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Connie Sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	18-MAR-2013
Filing Date:	28-MAR-2012
Time Stamp:	14:40:11
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1930
RAM confirmation Number	1378
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

<table>
<tr><td>1</td><td></td><td>PRP.pdf</td><td>564023
946e617b3edb44d50d0b6bd408d2bfa7431cdb91</td><td>yes</td><td>8</td></tr>
<tr><td rowspan="4"></td><td colspan="5"><b>Multipart Description/PDF files in .zip description</b></td></tr>
<tr><td colspan="3"><b>Document Description</b></td><td><b>Start</b></td><td><b>End</b></td></tr>
<tr><td colspan="3">Receipt of Petition in a Reexam</td><td>1</td><td>7</td></tr>
<tr><td colspan="3">Reexam Certificate of Service</td><td>8</td><td>8</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>2</td><td>Fee Worksheet (SB06)</td><td>fee-info.pdf</td><td>30354
176b48309b29110f42cb55639d018c4bc022fde3</td><td>no</td><td>2</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td colspan="4"><b>Total Files Size (in bytes):</b></td><td colspan="2">594377</td></tr>
</table>

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

TRANSMITTAL LETTER

Enclosed please find the following:

1. Patent Owner's Response to Office Action of January 16, 2013 (56 pages);
2. Declaration of Angelos D. Keromytis, Ph.D. (11 pages);
3. Appendix - List of Exhibits (1 page);
4. Exhibits Listed on Appendix;
5. Petition Seeking Waiver of 37 C.F.R. § 1.943 for Patent Owner's Response to Office Action of January 16, 2013 (2 pages);
6. Petition Fee of $1,930; and
7. Certificate of Service (2 pages).

Please grant any extension of time and charge any required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 18, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the Patent Owner certifies that copies of the following documents:

1. Transmittal Letter (1 page);
2. Patent Owner's Response to Office Action of January 16, 2013 (56 pages);
3. Declaration of Angelos D. Keromytis, Ph.D. (11 pages);
4. Appendix - List of Exhibits (1 page);
5. Exhibits Listed on Appendix;
6. Petition Seeking Waiver of 37 C.F.R. § 1.943 for Patent Owner's Response to Office Action of June 4, 2012 (2 pages); and
7. Certificate of Service (2 pages)

were served by first-class mail on March 18, 2013 on counsel for the third-party Requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 18, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U.S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S RESPONSE TO OFFICE ACTION OF JANUARY 16, 2013

On June 4, 2012, the U.S. Patent and Trademark Office ("Office") issued a first Office Action ("First OA" or "First Office Action") in these reexamination proceedings. VirnetX Inc. ("VirnetX" or "Patent Owner"), the owner of U.S. Patent No. 8,051,181 ("the '181 patent"), filed a Response ("Response") on September 4, 2012. Requester Apple Inc. ("Apple" or "Requester") filed Comments ("Comments") on October 22, 2012. On January 16, 2013, the Office issued a second Office Action ("Second OA" or "Second Office Action"), which was designated an Action Closing Prosecution ("ACP"), in these proceedings.

Claims 1-29 are patentable at least for the reasons that follow and the reasons stated in VirnetX's September 4, 2012, Response. Thus, VirnetX requests that claims 1-29 be confirmed. This Response is supported by a Supplemental Declaration of Angelos D. Keromytis, Ph.D. ("Supp. Keromytis Decl."), and at times, this Response also refers to the initial Declaration of Angelos D. Keromytis, Ph.D. ("Keromytis Decl.") filed on September 4, 2012. The Supplemental Declaration is necessary and was not earlier presented because Patent Owner must address, among other things, the new rejections presented by the Office in the ACP that were not present in the First Office Action, as described in further detail below. 37 C.F.R. § 1.116(e). Additional "good and sufficient reasons" are set forth in Patent Owner's concurrently filed Petition to Reopen Prosecution, which explains that the

Second Office Action should not have been an ACP, given the new rejections adopted by the Office. *Id.*

I. The Rejection of Claims 1-12, 14, 15, and 17-29 Based on *Beser* Should Be Withdrawn (Issue 1)

The Second Office Action rejects claims 1-12, 14, 15, and 17-29 under 35 U.S.C. § 102(e) based on *Beser*. (Second OA at 5.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. Independent Claim 1

1. *Beser* Fails to Disclose the Recited Features of "a First Device," "a Second Device," and "a Message from [the] Second Device of the Desire[] to Securely Communicate with the First Device"

Independent claim 1 recites a combination of features that pertain to the claimed "first device" and the claimed "second device." In particular, independent claim 1 requires both "receiving, at a network address corresponding to the secure name associated with *the first device*, a message *from a second device* of the *desire[] to securely communicate* with the first device" and also "sending a message over a secure communication link *from the first device to the second device*" (emphases added). Thus, independent claim 1 requires that both:

1. a message *of the desire to securely communicate* with the first device is received *from the second device to* a network address corresponding to the secure name associated with *the first device*, and
2. another message is sent *over a secure communication link from the first device to the second device*.

Beser does not disclose these features for at least the reasons discussed in the Response. (*See, e.g.*, Response at 7-10.) The Office's and Requester's assertions to the contrary are fundamentally flawed because they are based on an incorrect claim construction that ignores entire portions of the claim's plain language, an incorrect application of anticipation law, and an misunderstanding of Patent Owner's arguments.

a. The Rejection Is Based on an Unreasonable Claim Construction

The Second Office Action summarizes the two claim limitations discussed above by stating that "[t]he Examiner agrees with the third party requestor, the claim merely requires a message, including an IP address, being sent between two devices ('first device'/'second device')." (Second OA at 18.) This is incorrect. Under the broadest *reasonable* interpretation, the Office gives the words of the claim their *plain meaning*, unless inconsistent with the specification. M.P.E.P.

§ 2111.01. The Office's construction does not even afford the claim terms their plain meaning as it simply ignores entire elements of the claim and the relationship between the claimed first device and second device. Moreover, the Office is also incorrect that the claims merely require "a message" to be sent between two devices at least because the claims clearly recite two different messages (see bullet points 1 and 2 above). Because it is based on an incorrect construction of the claim limitations discussed above, and because it completely ignores the plain language of the claims, the rejection cannot be maintained. *See id.* § 2131 (to anticipate a claim, a reference must teach every element of the claim).

b. The Rejection Is Based on an Incorrect Application of Anticipation Law

In its Response, Patent Owner pointed out that the First Office Action, which adopted the request for reexamination ("Request"), never identified the alleged first device and the alleged second device in *Beser*. (Response at 9-10.) Instead, the First Office Action incorrectly mixed and matched among four different devices in *Beser* (first and second network devices 14 and 16 and end-point devices 24 and 26) in an attempt to show unpatentability. Now, rather than identifying which two of these four devices in *Beser* are the claimed first and second devices, the Office and Requester try to justify their previous analysis by stating that "the telephony, network devices (e.g., edge routers) and/or trusted third party network device described in *Beser* may, ***at any particular point***, be a 'first' or 'second' device in the claims." (Second OA at 17, quoting Comments at 4, emphasis added.)[1]

In other words, the Office and Requester assert that they can choose one device in *Beser* to read on "first device" for one claim recitation, but then later choose another device in *Beser* to read on the *same* "first device" for another claim recitation. They are incorrect. An anticipation rejection requires that the cited reference disclose all of the claimed features *arranged in the way that they are claimed*. *See* M.P.E.P. § 2131. By picking and choosing among different devices in *Beser* to read on the claimed first and second devices "***at any particular point***" (Second OA at 17, quoting Comments at 4, emphasis added), the Office and Requester have run afoul of this requirement.

[1] Requester's Comments later suggest that the Office has identified end-point devices 24, 26 in *Beser* as being the first and second devices. (Comments at 5.) First, this is inconsistent with the portion of the Comments quoted above. Second, the Office never adopted this position. (Second OA at 18-19.) And third, Patent Owner already explained in its Response that end-point devices 24, 26 cannot be the claimed first and second devices and still meet the remaining features recited in claim 1. (Response at 9-10.)

As a corollary to its incorrect argument about picking and choosing among different devices in *Beser*, the Office and Requester assert that the claimed "first device" can be interpreted to be *both* first network device 14 and end-point device 24 in *Beser*. (*Id.* at 18, quoting Comments at 5, "[i]t is also immaterial whether the 'first device' is considered to be the telephony device [16], the edge router [24] or both working together – *there is no restriction on the claims to this extent*," emphasis added.) This is incorrect because the claims *do include such a restriction*. Namely, the claims require that particular actions be performed by "the first *device*" and "the second *device*" (emphases added). Yet *Beser*'s first network *device* 14 is clearly a different *device* than end-point *device* 24. (*See Beser* Fig. 1.) Moreover, incorporating first network device 14 and end-point device 24 into a single device would render *Beser*'s tunneling scheme, which hides the IP address of end-point device 24, ineffective. (Second Keromytis Decl. ¶ 6.)

The Office and Requester still have not pointed to two devices in *Beser* that read on the recited first and second devices by meeting the two claim limitations discussed above. Indeed, Patent Owner has already explained how no combination of the first and second network devices (14, 16) and end-point devices (24, 26) can have all of the features of the recited first device and second device. (*See* Response at 9-10.) As such, the rejection should be withdrawn.

c. The Rejection Relies on Requester's Mischaracterization of Patent Owner's Arguments

Requester asserts that Patent Owner argued in its Response that the presence and reliance on intermediate devices between the alleged first device and the alleged second device distinguished the claims over *Beser*. (Comments at 4.) Patent Owner never made this argument and disputes Requester's characterization of Patent Owner's arguments. Instead, Patent Owner argued that the Office and Requester never identified an alleged first device and second device to begin with, and that none of the various different messages in *Beser* (e.g., request 112, inform 114, and negotiate 118) could read on the claimed "message of the desire[] to communication securely" while still possessing the remaining features recited in claim 1. (Response at 7-9.)

Rather than identifying the alleged first and second devices and the alleged message of a desire to securely communicate in *Beser*, Requester simply mischaracterizes Patent Owner's arguments as something that they are not. This does not sidestep the fact that the Office and Requester still have not shown that *Beser* anticipates claim 1. Because the Office and Requester have failed to meet their burden of showing that *Beser* discloses the "first device," the "second device," and "receiving, at a network address corresponding to the secure name associated with the first device, a message from [the] second device of the desire[] to securely communicate with the first device," as recited in claim 1, the rejection should be withdrawn and the claim should be confirmed.

2. *Beser* Fails to Disclose "Sending a Message over a Secure Communication Link from the First Device to the Second Device"

Claim 1 also recites, among other things, "sending a message over a secure communication link from the first device to the second device." Because, as discussed above, *Beser* does not disclose a first device and a second device that meet the requirements of claim 1, *Beser* also cannot disclose sending a message over a secure communication link *from the first device to the second device.* Additionally, as explained in the Response, *Beser* does not disclose this feature because (1) the broadest reasonable interpretation of "secure communication link" requires encryption, and *Beser*'s tunneling association is not encrypted; and (2) even if the Office maintains that a secure communication link does not require encryption, *Beser*'s tunneling association still is not a secure communication link. (*Id.* at 10-12.) The Office does not appear to take a stance on whether "secure communication link" requires encryption, but instead asserts that *Beser* teaches a secure communication link under both possible constructions. (Second OA at 19-21.) Patent Owner disagrees for the reasons stated in the Response and in the subsections below.

a. *Beser* Does Not Disclose that the Alleged Message from the First Device to the Second Device Is Encrypted

As explained in the Response, *Beser* teaches away from using encryption in its tunneling system. (Response at 11.) The Office disagrees, citing a new portion of *Beser* and asserting that "*Beser* specifically teaches utilization of encryption in combination with the tunneling, where this tunneling is being used as an additional means of making the channel for transmission secure, yet used in combination with legacy encryption to ensure data security (see column 2, lines 1-16)." (Second OA at 20.) When considered in its proper context, the cited portion of *Beser* supports Patent Owner's point that *Beser* teaches away from incorporating encryption into its tunneling scheme.

The newly cited portion is from *Beser*'s "Background of the Invention" section, which includes three separate paragraphs discussing three different prior art communication methods, each of which includes encryption. (*Beser* 1:54-2:35.) But *Beser* ends each of these paragraphs by explaining how the use of encryption in these systems is undesirable because of an *increased computational burden*. (*See, e.g.*, *id.* at 1:58-67, 2:12-17, 2:33-35; *see also* Supp. Keromytis Decl. ¶ 7.) After repeatedly and consistently associating encryption in these prior art systems with an *increased computational burden*, *Beser* includes a "Summary of the Invention" section, where *Beser* discloses that "[t]he method and system described herein may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication *without an increased computational burden*," i.e., without encryption. (*Beser* 3:4-9, emphasis added.) *Beser* also discloses that the addresses of the ends of the tunneling association are "hidden" not using encryption, but instead using the "negotiation" process of step 118 that ensures that the addresses of the ends of the VoIP association are not included in the data packet address fields. (*See, e.g.*, *id.* at 11:59-12:16; Supp. Keromytis Decl. ¶ 7.)

Another portion of the Second Office Action also asserts that *Beser*'s tunneling associations use encryption, (Second OA at 23, citing *Beser* 11:22-25), but this is incorrect. In the cited portion, *Beser* discloses that "IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." (*Beser* 11:22-25.) But the "IP 58 packets" being described in this portion of *Beser are not a part of the alleged secure communication link.* Instead, the "IP 58 packets" described in *Beser* are sent as part of step 114, which is a communication between first network device 14 and *trusted-third-party network device 30*, as evidenced by reading the entirety of the paragraph to which the Comments cite, rather than the single out-of-context sentence quoted by Requester. (*Id.* at 11:9-25.) Thus, this communication is not sent between the alleged first device and the alleged second device, which, as discussed above, the Office and Requester have incorrectly asserted is some combination of network devices 14, 16 and end-point devices 24, 26. (Supp. Keromytis Decl ¶ 8.) Accordingly, the portion of *Beser* that the Office points to as allegedly teaching encryption has *nothing to do with the alleged secure communication link* and fails to support the rejection.

b. Even If a Secure Communication Link Did Not Require Encryption, *Beser* Still Does Not Disclose One

Additionally, for at least the reasons presented in the Response, *Beser*'s tunneling scheme still does not disclose a secure communication link, even if the Office incorrectly determines that a secure communication link does not require encryption. (Response at 12.) For example, as discussed in the Response, *Beser*'s tunneling scheme does not secure communications from eavesdropping once the originating and terminating ends have been discovered. (*Id.*) In contrast, the '181 patent specifically distinguishes communications that incorporate "data security" and are thus "immune to eavesdropping" from communications that merely "prevent an eavesdropper from discovering that [a] terminal . . . is in communication with [another] terminal." (*Id.*)

In view of the above, *Beser* does not disclose "sending a message over a secure communication link from the first device to the second device" and cannot anticipate claim 1.

B. Independent Claim 2

Independent claim 2 recites, among other things, "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." As discussed above and in the Response, *Beser* does not disclose that its tunneling scheme includes a secure communication link and thus cannot anticipate claim 2.

C. Dependent Claim 4

Dependent claim 4 recites that "the secure name indicates security." *Beser* does not disclose this feature. The Office and Requester assert that *Beser*'s "unique identifier" discloses a secure name. (Req. at 32.) *Beser* discloses that the unique identifier may include a dial-up number, e-mail address, domain name, employee number, social security number, driver's license number, previously assigned IP address, etc. (*Beser* 10:37-11:8.) But none of these examples indicate anything about security. The Office and Requester cite a portion of *Beser* describing encrypting IP packets between a first network device 14 and trusted-third-party network device 30. (Req. at 36, citing *Beser* 11:13-25.) While *Beser* discloses that the encrypted packets may include a unique identifier, this passage simply does not disclose that the unique identifier, itself, indicates security. And the rest of *Beser* does not disclose that the unique identifier indicates anything about security. Thus, *Beser* does not anticipate claim 4.

D. Dependent Claim 5

Dependent claim 5 recites that "receiving the message containing the network address associated with the secure name of the second device includes *receiving the message in encrypted form*" (emphasis added). As discussed in the Response, *Beser* does not disclose that the alleged message containing the network address is received in encrypted form. (Response at 13.) The Office and Requester disagree, asserting *Beser* discloses that "[t]he IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." (Second OA at 23; Comments at 8, both quoting *Beser* 11:22-25.) This is incorrect because the cited portion of *Beser* has nothing to do with the alleged message containing the network address.

When analyzing claim 2, from which claim 5 depends, the Office and Requester assert that the negotiation step 118 of *Beser* corresponds to the alleged "message containing the network address." (*See* Req. at 34, "[f]ollowing *the negotiation*, the first device (14)—the requesting device—has obtained 'the following network addresses . . . ,'" emphasis added.) But the cited passage in *Beser* has nothing to do with the negotiation step 118. Instead, as discussed above, the "IP 58 packets" described in this portion of *Beser* are sent as part of step 114, which is a different message altogether from step 118. (*See Beser* 11:9-25, directed entirely to the communication sent as a part of step 114; *see also id.* at Fig. 6, showing steps 114 and 118 as different communications.) Thus, the cited passage fails to support the rejection.

Moreover, claims 2 and 5 together require that the message containing the network address be received in encrypted form *by the first network device*. The message in step 114 is received by trusted-third-party network device 30, not by the alleged first device. Thus, the message in step 114 cannot be the message recited in claim 5. In view of the above, *Beser* does not anticipate claim 5.

E. Independent Claims 24, 26, and 29

Although of different scope, independent claims 24, 26, and 29 recite features similar to those discussed above in connection with independent claim 1, as discussed in Patent Owner's previous Response. (Response at 16-19.) Thus, for reasons similar to those discussed above with respect to claim 1, and for the reasons set forth in the previous Response, *Beser* does not anticipate claims 24, 26, and 29. (*Id.*)

F. Independent Claim 28

Although of different scope, independent claim 28 recite features similar to those discussed above in connection with independent claim 2, as discussed in Patent Owner's previous Response. (*Id.* at 18.) Thus, for reasons similar to those discussed above with respect to claim 2, and for the reasons set forth in the previous Response, *Beser* does not anticipate claim 28. (*Id.*)

G. Dependent Claims 3, 6-12, 14, 15, 17-23, 25, and 27

Claims 3, 6-12, 14, 15, 17-23, 25, and 27 each ultimately depend from one of independent claims 2, 24, and 26, and include all of the features of the independent claim from which they depend. Accordingly, claims 3, 6-12, 14, 15, 17-23, 25, and 27 are patentable over *Beser* for at least the reasons discussed above with respect to claims 2, 24, and 26.

In view of the above, the rejection of claims 1-12, 14, 15, and 17-29 based on *Beser* should be withdrawn and the claims should be confirmed.

II. The Rejection of Claims 1, 2, 7-9, 12-17, 19-21, and 24-29 Based on *Mattaway* Should Be Withdrawn (Issue 3)

The Second Office Action rejects claims 1, 2, 7-9,[2] 12-17, 19-21, and 24-29 under 35 U.S.C. § 102(e) based on *Mattaway*. (Second OA at 5-6.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

[2] Patent Owner notes that Requester additionally proposed rejections of claims 5 and 6 in its Request. However, the Second Office Action does not reject claims 5 and 6 based on *Mattaway*. (*See* Second OA at 5-6.) Thus, Patent Owner understands that the Office has not rejected those claims in view of *Mattaway*.

A. Independent Claim 1

1. *Mattaway* Fails to Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire[] to Securely Communicate with the First Device"

Independent claim 1 recites, among other things, "receiving, at a network address corresponding to the secure name associated with *the first device, a message from a second device of the desire[] to securely communicate* with the first device" (emphasis added). The Office and Requester have changed their position with regard to what in *Mattaway* allegedly discloses this feature. As discussed below, both the old position and the new position are incorrect.

The First Office Action, adopting the Request, asserted that the <CONNECT REQ> message in *Mattaway* disclosed the recited "message . . . of the desire[] to securely communicate." (First OA at 5, incorporating Req. at 68-94.) The Office and Requester cited to two different protocols in *Mattaway*, and for each protocol focused on the <CONNECT REQ> message as allegedly disclosing the recited "message . . . of the desire[] to securely communicate." (Req. at 70-71, citing *Mattaway* 18:41-45 and Fig. 16A as disclosing processing a <CONNECT REQ> message in the alleged first protocol; Req. at 71, citing *Mattaway* 8:25-44 as disclosing processing a <CONNECT REQ> message in the alleged second protocol.) Now, the Second Office Action takes a new position presented for the first time in Apple's Comments on VirnetX's Response, asserting that *Mattaway*'s <CALL> message corresponds to the recited "message . . . of the desire[] to securely communicate." (Second OA at 34, "the process described in column 24, line 11 through 25, line 34, explains the callee receiving a request to communicate[] from the caller, to which the callee can either <REJECT>, or accept (<CALL ACK>) the call thereby establishing the connection.") *Mattaway* 24:11-25:34, as cited by the Office and Requester, deals exclusively with processing the <CALL> message sent between two webphones and has nothing to do with the <CONNECT REQ> message.

Neither *Mattaway*'s <CONNECT REQ> message nor its <CALL> message discloses "receiving, at a network address corresponding to the secure name associated with *the first device, a message from a second device of the desire[] to securely communicate* with the first device," as recited in claim 1 (emphasis added). Each message is discussed in turn below.

The <CONNECT REQ> message does not disclose the recited "message . . . of the desire[] to securely communicate" for at least two reasons. First, the <CONNECT REQ> message is not received "at a network address corresponding to the secure name associated with *the first device*" (emphasis added). The Office and Requester assert that *Mattaway*'s first processing unit 12 (the "caller" WebPhone in the *Mattaway* system) corresponds to the claimed first device:

> Upon retrieval of the IP address of the callee, "*the first processing unit 12 may then directly establish the point-to-point internet communications* with the callee using the IP address of the callee." . . . Thus, *Mattaway* discloses "sending a message over a secure communication link *from the first device* to the second device."

(Req. at 72, emphases added, internal quotation marks omitted.) But the <CONNECT REQ> message is received by mail server 28 or global server 1500, and not by the alleged first device. (*Mattaway* 7:63-65, "the first processing unit 12 sends a <ConnectReq> message via E-mail over the Internet 24 *to the mail server 28*," emphasis added; *id.* at 18:48-51, "Connection server 1512 remains in an idle state until a <CONNECT REQ> packet is transmitted from a WebPhone client *to global server 1500*," emphasis added.) Figs. 2 and 17A of *Mattaway*, reproduced below, also illustrate that the <CONNECT REQ> message is received by either mail server 28 or global server 1500, and not by the alleged first device.

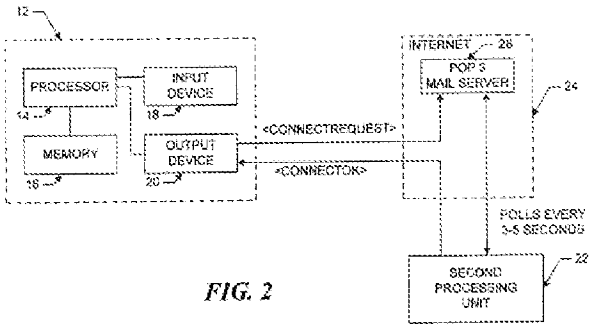


FIG. 2

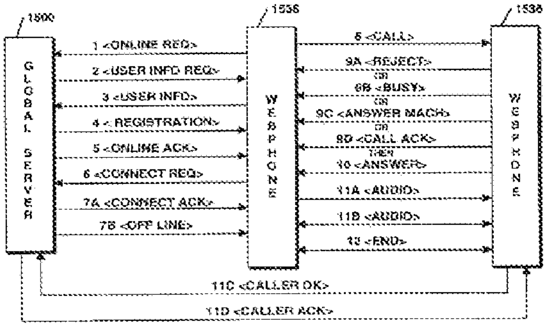


Figure 17A

Second, the <CONNECT REQ> message does not disclose the recited message because it is not a message "of the desire[] to securely communicate." In fact, the <CONNECT REQ> message does not include any information related to security. Tables 6 and 8 of *Mattaway* explain that a <CONNECT REQ> message includes the following data entries, along with a brief explanation of what is included in each data entry:

Data Entry	Comment
WPP_CONNECTREQ	WPP message identifier
Sid	Session ID
Version	Version of the webphone
callType	Call type 0:EMAIL/1:IPCALL
partyEmailAddr	E-mail address of person to call
email Addr	E-mail address of caller
IPAddr	IP Address

Data Entry	Comment
connectState/connectStatus	0: No Webphone; 1: Online; 2: Offline; 3: Reconnect; 4: Perm_Reconnect

(*Id.* at 36:45-65, 39:1-35, showing Tables 6 and 8.) None of the data entries included in the <CONNECT REQ> mention anything about security and, thus, the <CONNECT REQ> message cannot be a message "of the desire[] to securely communicate." (Supp. Keromytis Decl. ¶ 9.)

The <CALL> message also does not disclose the recited message because it also is not a message "of the desire[] to securely communicate." Tables 6 and 8 of *Mattaway* also explain that a <CALL> message includes the following data entries:

Data Entry	Comment
WPP_CALL	WPP message identifier
Sid	Session ID
Version	Version of the webphone
email Addr	E-mail address of caller
IPAddr	IP Address
Userinfo	FirstName, LastName, alias, emailAddr, street, apt., city, state, country, postalCode, phone, fax, company

Just like those included in the <CONNECT REQ> message, the data entries in the <CALL> message also indicate nothing about security. (*Id.*) Because the <CALL> message is silent regarding security, it also cannot be the recited message "of the desire[] to securely communicate."

2. *Mattaway* Fails to Disclose "a First Device Associated with a Secure Name and an Unsecured Name"

Claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." For the reasons provided in the Response and those discussed below, *Mattaway* does not disclose these features.

First, *Mattaway* does not disclose a "secure name." As explained in the Response, "secure names" are those names used to communicate securely that are resolved by a secure name service (i.e., a service that both resolves a name into a network address and further supports establishing a secure communication link). (*See, e.g.*, Response at 45-46.) The connection server 26 in *Mattaway*, however, is a conventional name server of the type distinguished by the '181 patent specification and does not qualify as a "secure name service" that can resolve "secure names." (Supp. Keromytis Decl. ¶ 10.) Instead, when provided with an e-mail address of a callee's device, connection server 26 merely returns an IP address, if one is associated with the e-mail address. (*Id.*; *Mattaway* 18:30-19:9, Fig. 16A.) *Mattaway* does not disclose that the connection server 26 provides any further support for establishing a secure communication link. (Supp. Keromytis Decl. ¶ 10.) Accordingly, its operation is conventional, it is not a "secure name service" in the context of the '181 patent, and the e-mail addresses disclosed in *Mattaway* are not "secure names." (*Id.*)

Second, *Mattaway* does not disclose that the alleged secure name—the encrypted e-mail address "eemailAddr" entry of Table 9—is associated with the alleged first device. (*Id.* ¶ 11.) As Requester points out, the "eemailAddr" entry is sent from the global server to the alleged first device, webphone 1536, as a part of the <USER INFO REQ> message. (Comments at 12; *Mattaway* 22:65-23:5, 40:27.) But *Mattaway* does not disclose that this "eemailAddr" entry is the e-mail address of the alleged first device or is at all associated with the alleged first device. (*Id.*) In fact, comparing the comments for the "eemailAddr" entry of Table 9, which read simply "encrypted email address," with the comments for the "emailAddr" entry of Table 8, which explain that it is the "email address *of [the] caller [i.e., the alleged first device*]" (emphasis added), makes it clear that the "eemailAddr" entry is different from the "emailAddr" entry included in the other messages. Moreover, there is simply no reason for the "eemailAddr" entry to be the encrypted e-mail address *of the alleged first device*, because this message is being sent *to* the alleged first device in between two messages from the alleged first device, <ONLINE REQ> and <USER INFO>, during which the alleged first device informs global server 1500 of its e-mail address. (*Mattaway* 22:47-23:5, Tables 6 and 8.) It would be unnecessary for global server 1500 to reply back to the alleged first device with the alleged first device's e-mail address after the alleged first device already provided that address to global server 1500. Thus, while *Mattaway* does not disclose the device to which the "eemailAddr" entry corresponds, it certainly does not disclose that it corresponds to the alleged first device.

In view of the above, *Mattaway* does not anticipate claim 1.

B. Independent Claim 2

Independent claim 2 recites, among other things, "a second device having a secure name" and "from [a] first device, sending a message to a secure name service." For at least the reasons in the response and those discussed above with regard to claim 1, *Mattaway* does not disclose a secure name or a secure name service. Thus, *Mattaway* does not anticipate claim 2.

C. Independent Claims 24, 26, 28, and 29

Although of different scope, independent claims 24, 26, 28, and 29 recite features similar to those discussed above in connection with independent claim 1, as discussed in Patent Owner's previous Response. (Response at 25-28.) Thus, for reasons similar to those discussed above with respect to claim 1, and for the reasons set forth in the previous Response, *Mattaway* does not anticipate claims 24, 26, 28, and 29. (*Id.*)

D. Dependent Claims 7-9, 12-17, 19-21, 25, and 27

Claims 7-9, 12-17, 19-21, 25, and 27 each ultimately depend from one of independent claims 2, 24, and 26, and include all of the features of the independent claim from which they depend. Accordingly, claims 7-9, 12-17, 19-21, 25, and 27 are patentable over *Beser* for at least the reasons discussed above with respect to claims 2, 24, and 26.

In view of the above, the rejection of claims 1, 2, 7-9, 12-17, 19-21, and 24-29 based on *Mattaway* should be withdrawn and the claims should be confirmed.

III. The Rejection of Claims 3, 4, 10, 11, 18, and 23 Based on *Mattaway* in View of *Beser* Should Be Withdrawn (Issue 4)

The Second Office Action rejects claims 3, 4, 10, 11, 18, and 23 under 35 U.S.C. § 103(a) based on *Mattaway* in view of *Beser*. (Second OA at 6.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. Dependent Claim 4

Claim 4 recites that "the secure name indicates security." The combination of *Mattaway* and *Beser* does not disclose or suggest this feature. *Mattaway* does not disclose this feature, and the Office and Requester do not allege that it does. (Req. at 96.) Instead, the Office and Requester allege that *Beser* discloses this feature, citing the same portion of *Beser* used to reject claim 4 in the anticipation rejection of Issue 1. (*Id.*) This is incorrect because *Beser* does not disclose that its unique identifier indicates security. Thus, *Beser* does not make up for the deficiencies of *Mattaway*.

Moreover, the Office's and Requester's obviousness analysis is deficient because it is based on nothing more than conclusory statements. The Office and Requester provide no reasoning beyond summarily concluding that "[a] person skilled in the art . . . would have immediately recognized the beneficial use of secure names that indicate security as disclosed by *Beser* would have been equally useful to those methods already described by *Mattaway*." (*Id.*) This is incorrect. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." (alteration in original) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); M.P.E.P. § 2141.III. Accordingly, the combination of *Mattaway* and *Beser* does not render claim 4 obvious.

B. Dependent Claim 10

Claim 10 recites "receiving the message [containing the network address associated with the secure name of the device] at the first device through tunneling *within the secure communication link*" (emphasis added). The combination of *Mattaway* and *Beser* does not disclose or suggest this feature. In its rejection of claim 2, from which claim 10 depends, the Office asserts that a message in *Mattaway* from connection server 26 to the first processing unit 12 is the claimed "message containing the network address." (First OA at 5, incorporating Req. at 68-94; Req. at 90.) But, as explained in the Response, this message is not received *through the alleged secure communication link*, because the Office and Requester assert that the secure communication link is a point-to-point communication between the WebPhone applications of first processing unit 12 and second processing unit 22. (Response at 29; Req. at 90.) Thus, even if *Beser*'s tunneling methods were combined with *Mattaway*'s system as proposed by the Office and Requester, the combination still would not disclose receiving the message "through tunneling *within the secure communication link*" (emphasis added), because that message is not sent through the alleged secure communication link in the first place. Accordingly, the combination of *Mattaway* and *Beser* does not render claim 10 obvious. (*See also supra* Section I.A.2, explaining that *Beser* does not disclose a secure communication link.)

C. Dependent Claims 3, 11, 18, and 23

Claims 3, 11, 18, and 23 each ultimately depend from independent claim 2 and include all of the features of that claim. Accordingly, claims 3, 11, 18, and 23 are patentable over *Mattaway* in view of *Beser* for at least the reasons discussed above with respect to the rejections of claim 2 based on *Beser* and based on *Mattaway*.

In view of the above, the rejection of claims 3, 4, 10, 11, 18, and 23 based on *Mattaway* in view of *Beser* should be withdrawn and the claims should be confirmed.

IV. The Rejection of Claims 10 and 11 Based on *Mattaway* in View of RFC 2401 Should Be Withdrawn (Issue 5)

The Second Office Action rejects claims 10 and 11 under 35 U.S.C. § 103(a) based on *Mattaway* in view of RFC 2401. (Second OA at 6-7.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. Dependent Claim 10

Claim 10 recites "receiving the message [containing the network address associated with the secure name of the device] at the first device through tunneling *within the secure communication* *link*" (emphasis added). The combination of *Mattaway* and RFC 2401 does not disclose or suggest this feature. In its rejection of claim 2, from which claim 10 depends, the Office asserts that a message in *Mattaway* from connection server 26 to the first processing unit 12 is the claimed "message containing the network address." (First OA at 5, incorporating Req. at 68-94; Req. at 90.) But, as explained in the Response, this message is not received *through the alleged secure communication link*, because the Office and Requester assert that the secure communication link is a point-to-point communication between the WebPhone applications of first processing unit 12 and second processing unit 22. (Response at 31; Req. at 90.) Thus, even if RFC 2401's tunneling methods were combined with *Mattaway*'s system as proposed by the Office and Requester, the combination still would not disclose receiving the message "through tunneling *within the secure communication link*" (emphasis added), because that message is not sent through the alleged secure communication link in the first place. Accordingly, the combination of *Mattaway* and RFC 2401 does not render claim 10 obvious.

B. Dependent Claim 11

Claim 11 depends from independent claim 2 and includes all of the features of that claim. Accordingly, claim 11 is patentable over *Mattaway* in view of RFC 2401 for at least the reasons discussed above with respect to the rejection of claim 2 in view of *Mattaway*, and because the Office does not allege that RFC 2401 makes up for the above-noted deficiencies of *Mattaway*.

In view of the above, the rejection of claims 10 and 11 based on *Mattaway* in view of RFC 2401 should be withdrawn and the claims should be confirmed.

V. The Rejections Based on *Lendenmann* Should Be Withdrawn (Issues 6-8)

A. The Rejection of Claims 1-9, 12-15, and 18-29 Based on *Lendenmann* (Issue 6) Should Be Withdrawn

The Office rejected claims 1-9, 12-15, and 18-29 under 35 U.S.C. § 102(b) based on *Lendenmann*. (Second OA at 7-8.) For at least the reasons discussed in Patent Owner's previous Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

1. Independent Claim 1

a. *Lendenmann* Does Not Disclose "a First Device Associated with a Secure Name and an Unsecured Name"

The Office is incorrect in maintaining that an X.500 name corresponds to a "secure name," while a DNS name corresponds to an "unsecured name." (*Id.* at 56-58.) Requester asserts that "secure name" and "unsecured name" should be defined solely by reference to the '181 patent prosecution history and to a prior reexamination of a different patent—U.S. Patent No. 7,188,180 ("the '180 patent"). (*Id.*) The Office appears to agree. (*Id.*) The Office also argues that a DNS name is unsecured because a DNS name "leav[es] the address unsecured and out in the open," while an X.500 is secure because it hides the address. (*Id.*) But the Office fails to properly interpret the claim, relies on incompatible features of *Lendenmann*, and rejects the claims based on an analysis that contradicts many of its other arguments in this proceeding. As a result, the rejection should be withdrawn.

(i) Requester and the Office Err in Interpreting "Secure Name" and "Unsecured Name"

Requester contends that a secure name should be defined by no more than whether it is stored in a secure name registry, and whether a conventional DNS can resolve it. (*Id.* at 57-58.) Requester reaches this conclusion solely by relying on the '181 patent prosecution history and a prior reexamination of the '180 patent, without considering the context of the specification itself. (*Id.*) The Office appears to agree. (Second OA at 58.) The result of Requester's incorrect analysis, however, is an implicit claim construction that removes all meaning of "secure" and "unsecured" from the claim terms. This claim construction also contradicts the portions of the '181 patent specification on which statements from the prosecution history and the prior reexamination were based. The rejections predicated on this deficient construction should be withdrawn. M.P.E.P. § 2258(I)(G) ("During reexamination, claims are given the broadest reasonable interpretation *consistent with the specification* . . . ." (emphasis added)).

The statements that Requester substitutes for the '181 patent specification in its claim interpretation analysis cannot bear the weight Requester places on them. (Second OA at 56-58.) For example, the quoted statements from the prosecution history of the '181 patent merely illustrate exemplary differences between a "secure name" and a "secure domain name" in response to an indefiniteness rejection under 35 U.S.C. § 112, second paragraph. (*See* Ex. A-28 at 9.) Similarly, Requester's out-of-context interpretation of the statements from the '180 patent reexamination contradicts the embodiments in the specification on which the statements from the '180 patent reexamination are based. (*See* Order at 5, citing '180 patent 51:25-35, corresponding to '181 patent 50:15-25.) These embodiments, relating to Figure 34, describe using a secure domain name for establishing secure communication links, while using unsecured names for non-secure communications. ('181 patent 48:50-52:58.) As just one example, the '181 patent specification describes replacing a top-level domain name with a secure domain name in order to establish a secure communication link. (*Id.* at 48:53-55, 50:7-59.) Afterwards, the '181 patent specification describes replacing the secure domain name with a non-secure domain name when the secure communication link is terminated. (*Id.* at 51:51-55.) Requester, by taking the prosecution history and prior reexamination statements out of their context, generates a strained and deficient claim interpretation that strips all plain meaning from the "secure" and "unsecured" claim terms and contradicts the '181 patent specification. M.P.E.P. § 2258(I)(G).

The rejection should be withdrawn because *Lendenmann*, under a reasonable claim interpretation properly reflecting the nexus between secure names and secure communications, does not disclose at least "a first device associated with a secure name and an unsecured name," as recited in claim 1. Indeed, Requester expressly admits that it is "fundamentally implausible" that a name qualifying as a "secure name" would not have any nexus with ensuring secure communications. (Comments at 23.) But the Office and Requester did not dispute that *Lendenmann* merely presents X.500 and DNS as alternative DCE-compatible naming schemes: "X.500 is an emerging global directory service standard, but the Internet domain name system (DNS) is an established industry standard. For interoperability purposes, GDS supports both X.500 and DNS transparently." (*Lendenmann* 21; Response at 33; Second OA at 56-58.) As detailed in Patent Owner's previous Response, X.500 and DNS perform the very same functions in *Lendenmann*'s distributed computing environment, and a separate Security Service facilitates security functions without regard to whether a X.500 or DNS name is employed. (Response at 33-35.) Neither the Office nor Requester relies on any *Lendenmann* passages or provide any other support reflecting any nexus between X.500 names and secure communications. (Second OA at 57-58; Comments at 20-21, 23.) Thus, because the maintained rejection depends on incorrectly reading "secure" and "unsecured" out of the claim, the rejection should be withdrawn.

(ii) The Office Errs in Concluding that X.500 Names Are "Secure" and DNS Names Are "Unsecured"

The Office also asserts that an X.500 name is secure because "the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address." (Second OA at 58.) The Office then asserts that a DNS name is unsecured because "if an Internet Address alone is used then a traditional DNS [i]s used to access, leaving the address unsecured and out in the open." (*Id.*) The Office is incorrect because *Lendenmann* does not disclose hiding Internet addresses or accessing Internet addresses outside of the DCE directory service.

First, *Lendenmann* does not disclose hiding Internet addresses. Rather, as the Office clearly states in another section of the Second Office Action, the CDS has a simple function in a client/server context: "when given a name, CDS *returns the network address* of the named resource." (*Id.* at 56, citing *Lendenmann* 21, emphasis added.) This happens regardless of whether an X.500 name or a DNS name is used, since the directory service supports both "for interoperability purposes." (*Lendenmann* 21.) Because the Office's rationale for concluding that an X.500 name corresponds to a "secure name" is contrary to the teachings of *Lendenmann*, the rejection should be withdrawn.

Second, *Lendenmann* does not disclose accessing Internet addresses outside of the DCE directory service. Rather, *Lendenmann* explains that both DNS and X.500 names are used *within* the DCE directory service: "There are two well-established schemes in place that DCE makes use of: CCITT X.500 [and] Internet Domain Name Service (DNS)." (*Id.* at 23.) The Office again provides no citation or support for its assertion that if a DNS name were used, a "traditional DNS [would be] used to access, leaving the address unsecured and out in the open." (*See* Second OA at 58.) Rather, *Lendenmann* utilizes both X.500 and DNS names within its DCE, and the Security Service performs its authentication and authorization features regardless of whether an X.500 or DNS name is used. (*Lendenmann* 34.)

The rejection based on *Lendenmann* should be withdrawn.

b. The Office Incorrectly Relies on Multiple Unrelated Features as Corresponding to the "First Device" Recited in Claim 1

The Office does not identify a single device within *Lendenmann* that satisfies all of the claim features recited for the "first device" in claim 1. Instead, the Office relies on a DCE cell as the "first device" for some features of claim 1, while relying on a specific server for other features of a "first device." Accordingly, the rejection of claim 1 should be withdrawn because the Office has failed to show how *Lendenmann* discloses "all of the limitations arranged or combined in the same way as recited in the claim." *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008).

In claim 1, the recited "first device" is associated with a secure name and an unsecured name. The Office asserts that a DCE cell corresponds to the "first device" and may be associated with an X.500 name as well as a DNS name due to cell-name aliasing. (Second OA at 56; *Lendenmann* 23-24, discussing "Cell Names.") A DCE cell is defined as "a group of users, systems and resources that are typically centered around a common purpose." (*Lendenmann* 20.) *Lendenmann* further states that "[e]ach cell is a self-sufficient, independently managed unit in a global distributed computing environment" that contains at least one Security Server, one CDS, and three DTS Servers per LAN. (*Id.* at 21.) The aliasing feature is limited to DCE cells. (*Id.*)

The "first device" is again recited in the claim 1 feature of "receiving, at a network address corresponding to the secure name associated with the *first device*, a message from a second device of the desire[] to securely communicate with the *first device*" (emphases added). For this feature of claim 1, the Office changes its position and relies not on a DCE cell as corresponding to the "first device," but rather a particular *Lendenmann* server. (Second OA at 59, citing Req. at 106-08.) The Office argues that a client device engaged in initiating a security-enhanced RPC (alleged to correspond to the "message . . . of the desire[] to securely communicate") sends a message to a server device that might specify the level of protection to be applied, which is all a continuation of the interaction between a client and a server host shown below. (*Id.*)

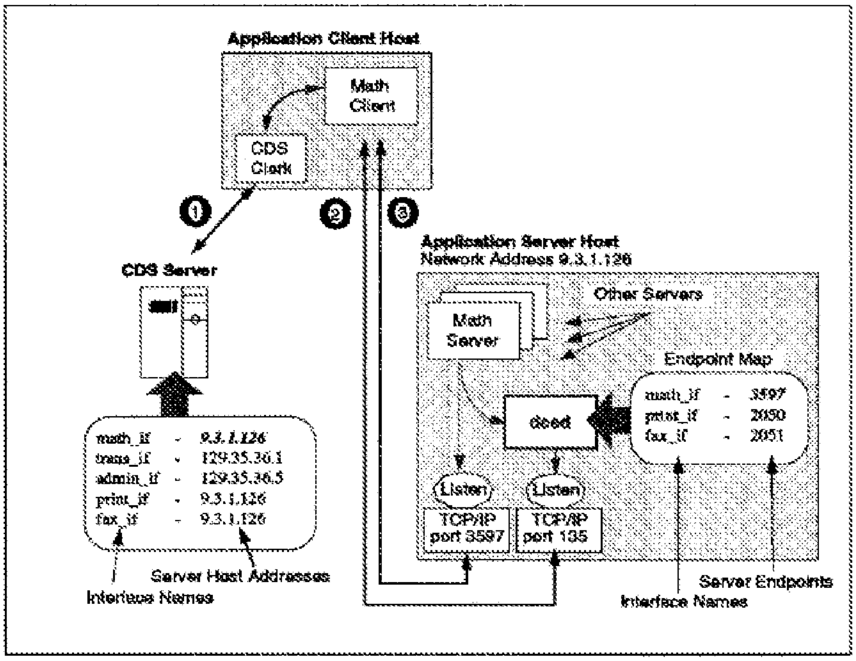


Figure 68. Steps Involved in Finding a Server

(*Lendenmann* 190; Second OA at 59, citing Req. at 106-08, reproducing *Lendenmann* 190.) Thus, the Office's argument that a server host device corresponds to the "first device" of claim 1 for the "receiving . . . a message" feature is inconsistent with the Office's contrary position that a DCE cell corresponds to the "first device" for other features of claim 1. (Second OA at 59, citing Req. at 106-08.)

Because the Office's rejection depends on at least two different entities corresponding to the "first device" for different features of claim 1, *Lendenmann* fails to anticipate. *Net MoneyIN*, 545 F.3d at 1371. Rather, the Office has incorrectly treated the claims "as mere catalogs of separate parts, in disregard of the part-to-part relationships set forth in the claims and that give the claims their meaning." *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010) (citation omitted). The rejection of claim 1 should therefore be withdrawn.

For all of the above reasons, in addition to those set forth in Patent Owner's previous Response, the rejection of claim 1 should be withdrawn. (Response at 33-35.)

2. Independent Claim 2

a. *Lendenmann* Does Not Disclose "Sending a Message to a Secure Name Service," "Receiving a Message Containing the Network Address," and "Sending a Message . . . Using a Secure Communication Link"

The Office relies on the RPC feature of *Lendenmann* as allegedly disclosing "sending a message using a secure communication link." (Second OA at 62-63; Req. at 114-15, quoting *Lendenmann* 192.) But for the earlier claim features of "sending a message to a secure name service" and "receiving a message containing the network address," the Office now relies on a non-RPC embodiment of *Lendenmann*. (Second OA at 62-63; Comments at 22.) Thus, the Office incorrectly mixes and matches different embodiments of *Lendenmann* to allegedly disclose the different claim features recited in claim 2, and the rejection should be withdrawn. *Net MoneyIN*, 545 F.3d at 1371.

The original proposed rejection for all of these three claim features relied on the RPC feature of *Lendenmann*. (*See, e.g.*, Req. at 112-13, citing *Lendenmann* 173-79; Req. at 113-14, citing *Lendenmann* 190-91; Req. at 114-15, citing *Lendenmann* 192.) Patent Owner traversed this rejection in part by explaining how the RPC binding process involves searching for servers based on criteria other than server names, and, therefore, *Lendenmann* does not disclose "sending a message . . . requesting a network address associated with the secure name of the second device." (Response at 37-39.) Patent Owner additionally traversed the original rejection by explaining, among other things, how a client obtains a list of *several compatible servers* during the RPC binding process, rather than receiving "a message containing the network address associated with the secure name of the second device," as recited in the claim. (*Id.* at 38-39.)

Requester did not contradict or contest Patent Owner's detailed arguments regarding the RPC binding process. (Comments at 22-23.) Neither did the Office. (Second OA at 61-63.) Instead, Requester and the Office now rely on a non-RPC feature of *Lendenmann* as allegedly showing the "sending a message to a secure name service" and "receiving a message" features of claim 2, rather than the RPC binding process. (Comments at 22; Second OA at 62-63, citing *Lendenmann* 21.) This revised argument, now relying on multiple embodiments for various features of claim 2, fails to support the rejection.

Lendenmann expressly differentiates between various types of communications in DCE. *Lendenmann* explains that its "OSF DCE components use three distributed computing models": (1) the client/server model, (2) the remote procedure call model, and (3) the data sharing model. (*Lendenmann* 8-9; Supp. Keromytis Decl. ¶ 13.) *Lendenmann* illustrates the client/server model as a request/response system of communication:

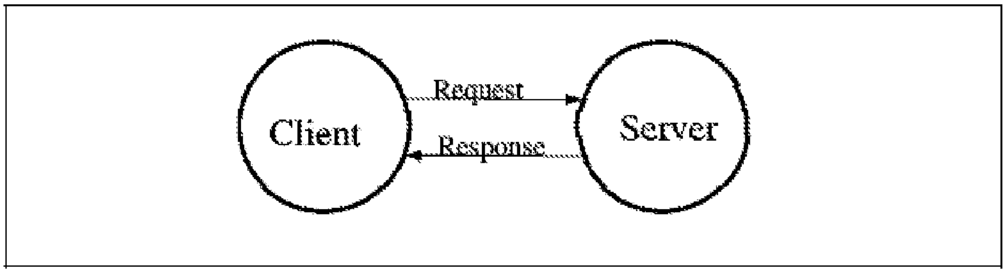


Figure 4. Client/Server Model

(*Lendenmann* 8.) The CDS-specific section of *Lendenmann* succinctly explains that the CDS "follows the client/server model." (*Id.* at 29.) It specifies that the CDS clerk "receives a request from [a] DCE application." (*Id.*) The CDS clerk then searches for the requested information. (*Id.* at 29-30.) Finally, the clerk "passes the requested data to the client application." (*Id.* at 30.) All of this language is consistent with the client/server model depicted in Figure 4, reproduced above. (*Id.* at 8; Supp. Keromytis Decl. ¶ 13.) Never is this simple lookup procedure referred to as an RPC or "data sharing" model communication.

In fact, this procedure in the CDS-specific section of *Lendenmann* is not described as an RPC because it stands in stark contrast to the binding process required for initiating RPCs. As described in Patent Owner's previous Response, the binding process involving the CDS during RPC setup identifies servers to the client based on functional criteria other than server names, whereas a CDS in the client/server model returns a network address "when given a name." (*Compare* Response at 37-38, citing *Lendenmann* 172-85, *with Lendenmann* 21.) Thus, these two embodiments—the client/server model and the RPC model—are incompatible because they use fundamentally different methods of resolving network addresses for use in DCE communications. (Supp. Keromytis Decl. ¶ 14.) The rejection should therefore be withdrawn.

Finally, the Office argues that with regard to "picking and choosing" arguments, "if these are all features available in Lendenmann, and if a combination of the features described in Lendenmann are usable together, then it properly rejects the claims." (Second OA at 63.) This is not the law. The Federal Circuit has repeatedly explained that a prior art reference "must clearly and unequivocally disclose the claimed [invention] or direct those skilled in the art to the [invention] without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference." *Net MoneyIN*, 545 F.3d at 1371 (alterations in original) (quoting *In re Arkley*, 455 F.2d 586, 587 (C.C.P.A. 1972)). The Office's reliance on multiple DCE communication models to correspond to the various features of claim 2 is the result of incorrectly mixing and matching selections of various features. (Response at 39.)

Because the Office relies on multiple, incompatible DCE communication models in *Lendenmann* to allegedly read on the various features of claim 2, the rejection should be withdrawn. (Comments at 22; Second OA at 61-63); *Net MoneyIN*, 545 F.3d at 1369, 1371.

b. *Lendenmann* Does Not Disclose a "Secure Name"

As discussed above in Section V.A.1.a.i, the Office and Requester incorrectly interpret "secure name" in a manner that is inconsistent with the specification. This interpretation, relying on out-of-context external statements, reads the term "secure" out of the plain claim language and fails to comport with the portions of the specification on which those external statements rely. Moreover, because *Lendenmann* merely discloses that X.500 and DNS names are alternatives to each other for cell-name aliasing, and because *Lendenmann* provides a separate security service that operates the same regardless of whether X.500 or DNS names are used, the X.500 and DNS names are neither secure nor unsecured, as explained in Patent Owner's previous Response. (*See* Response at 33-36.) Thus, the rejection of claim 2 should be withdrawn.

c. *Lendenmann* Does Not Disclose a "Second Device"

The Office incorrectly mixes and matches features of *Lendenmann* as corresponding to the "second device" of claim 2 for different features of the claim. For instance, the Office identifies only a DCE cell as potentially having an X.500 name—the alleged "secure name" in claim 2. (Req. at 111, relying on *Lendenmann* 23, discussing "Cell Names.") A DCE cell is defined as "a group of users, systems and resources that are typically centered around a common purpose." (*Lendenmann* 20.) *Lendenmann* further explains that "[e]ach cell is a self-sufficient, independently managed unit in a global distributed computing environment" that contains at least one Security Server, one CDS, and three DTS Servers per LAN. (*Id.* at 21.)

But for the features of sending and receiving "a message" in other portions of claim 2, the Office relies on a particular server (not a DCE cell) as corresponding to the claimed "second device." (Req. at 112-15, citing Fig. 68, reproduced above in Section V.A.1.b.) So again, the Office has not shown how *Lendenmann* discloses "all of the limitations arranged or combined in the same way as recited in the claim." *Net MoneyIN*, 545 F.3d at 1371; *Therasense*, 593 F.3d at 1332. The Office's "picking and choosing" in rejecting claims under 35 U.S.C. § 102 is also incorrect for the reasons stated above, including that it contradicts both *Net MoneyIN*, 545 F.3d at 1371, and *In re Arkley*, 455 F.2d at 587.

d. *Lendenmann* Does Not Teach a "Secure Name Service"

Requester interprets a "secure name service" as requiring nothing more than a name service capable of resolving a secure name, pronouncing its interpretation the "broadest reasonable construction." This analysis, however, relies exclusively on the '181 patent prosecution history and a prior reexamination of the '180 patent for its claim construction arguments, (*see* Comments at 21-22), which is incorrect for the reasons discussed above. Because the resulting interpretation is not consistent with the specification, the rejection should be withdrawn. M.P.E.P. § 2258(I)(G).

In fact, Requester's claim interpretation contradicts the embodiments in the patent specification on which the statements from the '180 patent reexamination are based. (*See* Order at 5, citing '180 patent 51:25-35, corresponding to '181 patent 50:15-25.) In this embodiment of the '181 patent specification, when the standard top-level domain name is replaced with the secure top-level domain name, "software module 3309 sends a query to SDNS 3313." ('181 patent 50:36-39, describing step 3408 of Fig. 34.) Then, in step 3409, "SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link." (*Id.* at 51:15-17.) Thus, the SDNS embodiment on which Requester's claim interpretation is ultimately based in fact actively coordinates with the VPN gatekeeper to establish a VPN communication link, and therefore "further support[s] establishing a secure communication link," as discussed in Patent Owner's previous Response. (Response at 36-37.) Requester's selective reliance on out-of-context external statements is incorrect, inconsistent with the specification, and insufficient to support the rejection.

The Office, meanwhile, argues that *Lendenmann* teaches a secure name service because "when the CDS (or GDS) is given a X.500 name it returns the network address of the named resource . . . [as] opposed to when provided with an Internet Domain Name." (Second OA at 61, citing *Lendenmann* 21.) The contrast the Office attempts to set up between the use of an X.500 name and an Internet Domain Name does not exist in *Lendenmann*. *Lendenmann* explains that in a client/server context, "when given a name, CDS returns the network address of the named resource," and does so for both the X.500 and DNS names that it supports "for interoperability purposes." (*Lendenmann* 21.) The Office provides no support from *Lendenmann* for its assertion that the CDS/GDS does something different when it is provided a DNS name, compared to when it is provided an X.500 name.

Because the rejection is based on an interpretation that incorrectly interprets the claim language and relies on a misreading of *Lendenmann*, the rejection should be withdrawn for the reasons set forth above and in Patent Owner's previous Response. (Response at 36-37.)

e. *Lendenmann* Does Not Teach "Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

Patent Owner traversed the original rejection by explaining how *Lendenmann* does not disclose any nexus between its security-related features and X.500 names, such as "sending a message to the network address *associated with the secure name* of the second device *using a secure communication link*." (*Id.* at 39.) Patent Owner additionally traversed the rejection by demonstrating that neither Requester nor the Office have shown that use of X.500 names in security communications would be inherent. (*Id.*, quoting *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999).)

Requester did not substantively address Patent Owner's arguments. Requester complains that Patent Owner "employs a fundamentally implausible reading of *Lendenmann*" by arguing that no nexus exists between RPC security features and X.500 names, (Comments at 23), but provides no basis in *Lendenmann* nor any declarations or other support for its arguments, e.g., such as to try to allegedly show that *Lendenmann* differentiates between its use of X.500 names and DNS names. (*But see Lendenmann* 21, explaining equivalent use of DNS and X.500 "for interoperability purposes.") Thus, Requester's arguments were nothing more than irrelevant attorney argument, and fail to support the rejection to the extent relied upon by the Office. (Second OA at 64.)

The Office also did not substantively address Patent Owner's arguments. Rather, the Office cites *Lendenmann* for the proposition that an RPC client can choose a level of protection for authenticated RPC. (*Id.*) The Office appears to contend that the allegedly resulting authenticated RPC corresponds to the "secure communication link" of claim 2. (*Id.*, quoting *Lendenmann* 192.) Yet even if one were to incorrectly assume that the Office has shown a "secure communication link," the Office has not demonstrated that *Lendenmann* discloses the rest of the claim features of "*sending a message to the network address associated with the secure name of the second device* using a secure communication link" (emphasis added). On these features, the Second Office Action is silent despite Patent Owner's detailed arguments traversing the rejection.

As a result, the Office has not shown that *Lendenmann* discloses each and every feature of claim 2, and the rejection should be withdrawn for the reasons set forth above and in Patent Owner's previous Response. (Response at 39.)

3. Dependent Claims 5 and 6

The Office maintains the rejection of dependent claims 5 and 6 because "Lendenmann has been clearly described as providing encrypted communication between devices." (Second OA at 65.) The Office's reasoning has no bearing on claim 5, which, when incorporating the relevant features from independent claim 2, recites "receiving the message *containing the network address associated with the secure name of the second device* . . . in encrypted form" (emphasis added). Nor does it have any bearing on claim 6, which depends from claim 5 and further recites "decrypting" such a message. The Office has not identified any encrypted messages containing network addresses in *Lendenmann*, and *Lendenmann* in fact discloses none. (*Id.*) Thus, the maintained rejection should be withdrawn for the reasons in Patent Owner's previous Response. (Response at 40-41.)

Meanwhile, Requester's arguments regarding RPC procedures are irrelevant because, as discussed above in Section V.A.2.a, the RPC communication model of *Lendenmann* does not involve requesting or returning network addresses associated with any particular secure name. (Comments at 24; Response at 40-41.) Rather, within RPC, a CDS identifies servers to the client based on functional criteria other than server names. (*See supra* Section V.A.2.a, Response at 37-38.) Because Requester's position would necessarily preclude *Lendenmann* from disclosing at least "the message requesting a network address" feature of claim 2, on which both claims 5 and 6 depend, Requester fails to remedy the Office's rejection. The rejection should be withdrawn.

4. Dependent Claim 21

The Office maintains the rejection of dependent claim 21, stating that "just because a device has a secure name does not alleviate the fact that it still has an internet address associated with it." (Second OA at 66.) The Office's reasoning again has no bearing on the claim, which does not recite any "internet address." Thus, the maintained rejection should be withdrawn for the reasons in Patent Owner's previous Response. (Response at 41.)

Moreover, Requester's arguments regarding cell-aliasing fail to reconcile the Office's reliance on both DCE cells and specific servers for the "second device" recited in claim 2, which claim 21 incorporates by virtue of dependency. (*See supra* Section V.A.2.c.) Thus, Requester again fails to remedy the Office's deficient rejection. The rejection should be withdrawn.

5. Independent Claim 24 and Dependent Claim 25

The Office's maintained rejection of claims 24 and 25 depends on the same claim interpretation issues that plague its rejections of claims 1 and 2, as discussed above. (Second OA at 67.) The rejection is confused further by arguing that regardless of whether X.500 or DNS is used, "all names in the network communication of Lendenmann are somewhat secure," apparently relying on the Office's incorrect interpretation of "secure name" and "unsecured name" to distinguish between X.500 and DNS names. (Second OA at 67; *see supra* Section V.A.1.a.) Thus, the rejections should be withdrawn for the reasons set forth above with respect to claims 1 and 2, as well as those set forth in Patent Owner's previous Response. (Response at 41-42.) In the alternative, a non-final office action is in order because the issues in this proceeding, including what the Office means by "secure" and "unsecured," remain far from settled. M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed.").

6. Independent Claim 26 and Dependent Claim 27

The Office maintains the rejections of claims 26 and 27 by agreeing with Requester that the DCE cell name aliasing feature discloses "an unsecured name associated with the first device" and "a secure name associated with the first device, wherein a unique network address corresponds to the secure name." The Office is incorrect.

Lendenmann does not disclose that an X.500 name has its own unique corresponding network address. The cell-aliasing feature of *Lendenmann* providing for X.500 and DNS naming, on which Requester appears to rely, does not provide for any unique network addresses corresponding to X.500 names. (*Lendenmann* 24.) And neither the Office nor Requester cite any authority stating otherwise. (*See* Comments at 25; Second OA at 68-69.)

In light of these deficiencies with *Lendenmann*, the Office changes its argument in the Second Office Action to now assert that an X.500 name *itself* is the recited "unique network address." (Second OA at 68, "The X.500 and domain names associated with a device in a Lendenmann scheme *thus comprise* both a[n] unsecure and a unique secret[] network address," emphasis added; *compare* Req. at 142.) Not only is this an implausible reading of *Lendenmann*, which describes the differences between names and network addresses, but it misreads claims 26 and 27.

Claim 26 (and claim 27 via dependency) recites two separate names—a "secure name" and an "unsecured name"—as well as "a unique network address correspond[ing] to the secure name." The Office's new argument attempts to conflate the "secure name" and "unique network address" claim terms. As a result, the Office's rejection is based on an alleged embodiment in which only two of the three recited claim features ("secure name," "unsecured name," and "unique network address correspond[ing] to the secure name") could possibly be present.

Moreover, similar to the deficiencies of the Office's arguments discussed above in Section V.A.2.c, the Office incorrectly relies on both a DCE cell and a specific server device at various times for the "first device" of claims 26 and 27. (Req. at 141-45, discussing cell aliasing and specific servers, e.g., in Fig. 68.) The Office has incorrectly treated the claims "as mere catalogs of separate parts, in disregard to the part-to-part relationships set forth in the claims and that give the claims their meaning." *Therasense*, 593 F.3d at 1332.

For these reasons as well as those set forth in Patent Owner's previous Response, the rejections should be withdrawn. (Response at 42.)

7. Independent Claims 28 and 29

Although of different scope, independent claims 28 and 29 recite features similar to those discussed above in connection with claims 1 and 2, as discussed in Patent Owner's previous Response. (*Id.* at 42-43.) Thus, for reasons similar to those described above with respect to claims 1 and 2, and for the reasons set forth in the previous Response, *Lendenmann* does not anticipate claims 28 and 29. (*Id.*)

8. Dependent Claims 3-9, 12-15, and 18-23

Claims 3-9, 12-15, and 18-23 depend directly or indirectly from claim 2 and include all of its features. Thus, they are patentable at least for the reasons discussed above, in addition to the reasons set forth in Patent Owner's previous Response. (*Id.* at 36-40.)

B. The Rejection of Claims 10, 11, 16, and 17 Based on *Lendenmann* in View of *Beser* Should Be Withdrawn (Issue 7)

Claims 10, 11, 16, and 17 depend directly or indirectly from claim 2 and include all of its features. The Office does not rely on *Beser* to remedy the deficiencies of *Lendenmann* with respect to claim 2. Thus, claims 10, 11, 16, and 17 are patentable at least for the reasons discussed above with respect to *Lendenmann* and claim 2, in addition to the reasons set forth in Patent Owner's previous Response. (*Id.* at 36-40, 43.)

C. The Rejection of Claims 10 and 11 Based on *Lendenmann* in View of RFC 2401 Should Be Withdrawn (Issue 8)

Claims 10 and 11 depend directly from claim 2 and include all of its features. The Office does not rely on RFC 2401 to remedy the deficiencies of *Lendenmann* with respect to claim 2. Thus, claims 10 and 11 are patentable at least for the reasons discussed above with respect to *Lendenmann* and claim 2, in addition to the reasons set forth in Patent Owner's previous Response. (*Id.*)

VI. The Rejection of Claims 1-15, 18-23, 28, and 29 Based on *Provino* Should Be Withdrawn (Issue 9)

The Second Office Action rejects claims 1-15, 18-23, 28, and 29 under 35 U.S.C. § 102(e) based on *Provino*. (Second OA at 8-10, 69-75.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. The Office's New Rejection Regarding *Provino*

In the Second Office Action, the Office adopted a new rejection related to *Provino*, shifting the focus from a domain name to an Internet address. The Request originally alleged that two different domain names in *Provino* are the claimed "secure name" and "unsecured name":

> Provino additionally discloses two names associated for each of the servers (items 31(S), for example) on Virtual Private Network 15, one being a secure name, i.e., the Domain name stored in the VPN Name Server 32, and one being an unsecured name, i.e., the Domain name stored in Name Server 17 at ISP 11.

(Req. at 168.) The Office adopted this portion of the Request in its First Office Action. (First OA at 8, "This rejection was proposed by the third party requester in the Request, and it is adopted with regard to claims 1-15, 18-23, 28, and 29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.").

In the Second Office Action, however, the Office now alleges that the claimed "secure name" does not correspond to "the Domain name stored in the VPN Name Server 32," but instead corresponds to an integer Internet address:

> Provino further teaches use of a secure name where the device [may] only establish a secure communication link upon receipt of the secure name (the integer Internet address which is registered on the VPN name server (see column 9, line 56 through column 10, lines 7, column 9, lines 17-27, and column 13, [lines] 26-67).

(Second OA at 71.) Because the Office has issued what is effectively a new rejection regarding *Provino* in the Second Office Action, that action should not have been an ACP. Even under this new interpretation of *Provino*, however, it does not anticipate the rejected claims.

B. Independent Claim 1

Patent Owner disagrees with the rejections of claim 1 for at least the following reasons.

1. The Rejection Does Not Clearly Identify the "First Device" and "Second Device"

Independent claim 1 recites, among other things, "a first device associated with a secure name and an unsecured name." As Patent Owner explained in its Response, Requester mixed and matched features from two different devices in its attempt to show unpatentability. (*See* Response at 47, quoting inconsistencies in the Request.) Requester now contends that a server 31(S) is the claimed "first device" and a device 12(m) is the claimed "second device." (Comments at 26-28.) The Office does not identify which device is first and which is second, (*see* Second OA at 74), but based on the Office's apparent agreement with Requester, Patent Owner assumes that the Office is also treating server 31(S) as the claimed "first device" and device 12(m) as the claimed "second device." If this interpretation is incorrect, Patent Owner requests that the Office issue a new office action clarifying the rejection.

2. *Provino* Does Not Disclose "a Network Address Corresponding to the Secure Name Associated with the First Device"

The Office now contends that the claimed "secure name" is "the integer Internet address which is registered on the VPN name server." (*Id.* at 71.) However, if this address is the claimed "secure name," it is not clear what the Office contends is the claimed "network address corresponding to the secure name." It appears that the Office is relying on the "integer Internet address which is registered on the VPN name server" as being both the "secure name" and the "network address corresponding to the secure name." The claims and specification, however, differentiate between those two terms, and the same "integer Internet address" cannot qualify as both. To contend otherwise effectively reads "receiving, at a network address corresponding to the secure name" out of the claim, as the Office's interpretation reduces that clause to either "receiving, at the secure name" or "receiving, at a network address," since the Office apparently equates the secure name and the network address. This is not a reasonable interpretation of the claim, which expressly requires both a "secure name" and "a network address corresponding to the secure name." Since the Office has not identified both a "secure name" and "a network address corresponding to the secure name," the anticipation rejection must be withdrawn.

3. *Provino* Does Not Disclose the Claimed "Unsecured Name"

The Office appears to rely on server 31(S) as the claimed "first device associated with a secure name and an unsecured name." (*See id.* at 74.) The Office contends that "Provino teaches the use of an unsecured name where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43)." (*Id.* at 69; *see also id.* at 71.) *Provino*, however, teaches that public domain name server 17 does not contain any names or addresses associated with server 31(S). It states that "nameserver 17 is not provided with integer Internet addresses for servers 31(S) and other devices which are in the virtual private network 15." (*Provino* 10:48-51, emphasis added.) Thus, "the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(S) which is to be accessed from that nameserver 17." (*Id.* at 10:52-55, emphasis added.) Since the public domain name server 17 does not contain any name associated with server 31(S) (the alleged "first device"), *Provino* cannot teach that domain name server 17 provides an unsecured name associated with the first device.

4. *Provino*'s System Is Essentially a Firewall-Based System Like Those Disparaged and Disclaimed in the '181 Patent Specification

Placing a conventional domain name server behind a firewall does not convert it from being conventional into a secure domain name server. As the '181 patent specification explains, a secure domain name server must possess additional functionality not present in a conventional domain name server, and it specifically distinguishes the invention from the functions of a conventional domain name server. (*See* Response at 45-46, explaining how the patent specification disparages systems like *Provino*'s and how the claims cannot be read to encompass those systems.) Without a secure domain name server, *Provino* cannot disclose secure names. Therefore, it does not disclose, teach, or suggest at least the claimed "first device associated with a secure name and an unsecured name," and "receiving, at a network address corresponding to the secure name associated with the first device."

C. Independent Claim 2

Similar to claim 1, independent claim 2 recites a device having a "secure name." For the reasons discussed above in Section VI.B.2, this feature is not disclosed in *Provino*. Claim 2 also recites a "secure name service," but since name servers 17 and 32 are both conventional name servers of the type distinguished by the '181 patent, they are not the claimed "secure name service." (*See supra* Section VI.B.4.)

D. Dependent Claims 3-15 and 18-22

Claims 3-15 and 18-22 depend directly or indirectly from claim 2 and include all of its features. They are patentable for at least the reasons discussed above regarding claim 2.

E. Dependent Claim 23

Claim 23 depends from claim 2 and is patentable for at least the reasons discussed above regarding that claim. Claim 23 also recites that "the secure name of the second device is a secure, non-standard domain name." As explained above, *Provino* discloses only conventional domain name functions and only resolves conventional domain names. Accordingly, *Provino* does not disclose the claimed "non-standard domain name."

F. Independent Claim 28

Like claim 1, independent claim 28 recites multiple instances of "secure name." This feature is not disclosed in *Provino* for the same reasons discussed above regarding claim 1. And like claim 2, claim 28 further recites a "secure name service." This feature is not disclosed in *Provino* for the same reasons discussed above regarding claim 2.

G. Independent Claim 29

Independent claim 29 recites multiple instances of "secure name." This feature is not disclosed in *Provino* for the same reasons discussed above regarding claim 1. Claim 29 also recites "receiving at a network address associated with a secure name of a first device a message from a second device requesting the desire[] to securely communicate with the first device." This feature is similar to claim 1's "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." Accordingly, it is not disclosed in *Provino* for the same reasons discussed above regarding the similar feature of claim 1.

In view of the above, the § 102(e) rejections of claims 1-15, 18-23, 28, and 29 based on *Provino* should be withdrawn.

VII. The Rejection of Claims 24-26 Based on *Provino* in View of *H.323* Should Be Withdrawn (Issue 10)

The Second Office Action rejects claims 24-26 under 35 U.S.C. § 103(a) based on *Provino* in view of *H.323*. (Second OA at 11.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. The Office Has Not Set Forth a Prima Facie Case of Obviousness

As explained above in Section VI.A, the Office revised its interpretation of the applicability of *Provino* to the rejected claims and issued a new rejection based on that new interpretation. The Office is presumably applying that new interpretation to its obviousness rejection for claims 24-26, but it has provided no explanation of the alleged interplay between that new interpretation and the alleged teachings of *H.323*. There is no explanation in the Second Office Action of how or why one of ordinary skill in the art would have combined *H.323* with *Provino* under the Office's new interpretation. Accordingly, the rejection is deficient on its face and must be withdrawn. Should the Office subsequently attempt to clarify its rejection, it should do so in a non-final office action that permits Patent Owner an adequate opportunity to respond.

B. A *Provino/H.323* Rejection Cannot Also Rely on Teachings from *H.235*

The Office appears to continue to rely on the teachings of *H.235* as though they are part of *H.323*. (*Id.* at 75-76.) But simply referencing another document is not sufficient to incorporate that document by reference. *See Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). Since Requester and the Office have not identified any instance where *H.323* incorporates *H.235* by reference (as opposed to merely referring to it), the obviousness rejection based on *Provino* and *H.323* cannot also be based on any teachings from *H.235*. If the Office intends to reject the claims based on *Provino*, *H.323*, and *H.235*, it should do so through a new Office Action that sets forth this particular combination of references and provides the required reasons why one of ordinary skill in the art would have combined those three references and how they allegedly teach the claimed invention. Until it does so, it has not set forth a prima facie case of obviousness for that three-reference combination and the rejection must be withdrawn.

C. Claims 24-26 Distinguish over Any Reasonable Reading of *Provino*, *H.323*, and *H.235*

While it is not clear how the Office contends the claims are obvious over *Provino* in combination with *H.323* by itself or also in combination with *H.235*, Patent Owner is not aware of any reasonable interpretation of those references that teaches all of the claimed features of claims 24-26. If the Office relies on *Provino*'s teachings for any of the claimed features that are similar to those recited in claims 1-15, 18-23, 28, or 29, they are not taught for the reasons discussed above in Sections VI.B and VI.C. And if the Office relies on *H.323*'s teachings for any of the claimed features similar to those addressed in Sections VIII.B.10 and VIII.B.11 below, they are not taught for the reasons discussed in those sections and the sections referenced therein. Patent Owner also maintains the distinctions identified in its September 4, 2012, Response on pages 49-51.

For at least these reasons, the § 103 rejections of claims 24-26 based on *Provino* and *H.323* should be withdrawn.

VIII. The Rejection of Claims 1-29 Based on the Combined *H.323* References Should Be Withdrawn (Issue 11)

The Second Office Action rejects claims 1-29 under 35 U.S.C. § 102(b) based on *H.323*. (Second OA at 11-12.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. Combining the Teachings of *H.323*, *H.225*, *H.235*, and *H.245* Is Improper

For a prior art document to incorporate another by reference, the Federal Circuit requires that it "cit[e] such material in a manner that *makes clear* that the material is effectively part of the host document as if it were explicitly contained therein." *Advanced Display*, 212 F.3d at 1282 (emphasis added). The alleged incorporating statements in *H.323* fall well short of this standard.

The Office relies on a statement in *H.323* that expressly conditions its listing of thirty-two separate documents: "The following ITU-T Recommendations and other references *contain provisions, which through reference in this text*, constitute provisions of this Recommendation." (Second OA at 78, quoting *H.323* 2, emphasis added.) *H.323* does not state that *all provisions* of the listed references are part of *H.323*—it states only that those references *contain provisions* that are part of *H.323* when referenced in the text. Despite the explicit limitations in this statement, the Office nevertheless asserts that it suffices to incorporate the listed documents in their entireties. (*Id.*) As a result, the Office effectively rewrites *H.323* to read: "The following ITU-T Recommendations and other references ~~contain provisions, which through reference in this text,~~ constitute provisions of this Recommendation." (*See H.323* 2; *see also* Comments at 29, similarly omitting the conditional language from its quotation.)

The *H.323* statement is far from the "broad and unequivocal language" of full incorporation by reference that Requester alleges. (Comments at 29.) In *Harari v. Lee*, cited by Requester to support its position, the incorporating language was "broad and unequivocal" because it was unconditional and unmistakable: "The disclosures of the two applications *are hereby incorporate[d] by reference*." 656 F.3d 1331, 1335 (Fed. Cir. 2011) (alteration in original) (emphasis added). The Court contrasted that language against other conditional language incorporating only the "relevant portions of the disclosures." *Id.* at 1336. The conditional language in *Harari* is similar to the *H.323* language, stating that the thirty-two listed documents merely "contain provisions, which through reference in this text, constitute provisions of this Recommendation." (*H.323* 2.) As a result, *H.323* fails to incorporate *H.225*, *H.235*, and *H.245* in their entireties under established Federal Circuit law. *Advanced Display*, 212 F.3d at 1282; *Harari*, 656 F.3d at 1335-36.

Requester's remaining arguments in its Comments similarly fail to demonstrate a clear, unequivocal intent in *H.323* to fully incorporate *H.225*, *H.235*, and *H.245* by reference. (*Compare* Comments at 29-30 *with Harari*, 656 F.3d at 1335 (interpreting "hereby incorporate[d] by reference").) Requester furthermore simply ignores the explicit "optional" and "mandatory" feature limitations in the *H.323* passages it cites. (Comments at 29-30.)

Because the maintained rejections are predicated on incorrectly combining all of these references in their entireties, the rejections should be withdrawn.

B. The Office's "Incorporation by Reference" Arguments Do Not Insulate Its Incorrect Mixing and Matching Analysis in Rejecting the '181 Patent Claims

Even if one were to incorrectly assume that all of the asserted references are incorporated by reference into *H.323*, this does not give the Office license to selectively pick and choose from among multiple embodiments in these various documents to allege disclosure of each of the different, particular elements recited in the '181 patent claims. *Net MoneyIN*, 545 F.3d at 1371 (quoting *Arkley*, 455 F.2d at 587). In *Arkley*, the Court determined that combining the features of two embodiments *from the same prior art document* could not be used to reject the claims as anticipated because "there [was] nothing in the teachings relied upon by the Patent Office which 'clearly and unequivocally' directs those skilled in the art to make this selection" of different embodiments. 455 F.2d at 587-88 (further elaborating that an anticipation rejection is improper if there is "*any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference"). The Office's maintained rejections, selectively picking and choosing from different embodiments across a variety of cited references, do not show that the inventions claimed in the '181 patent are "*identically* disclosed or described in the prior art" as required under 35 U.S.C. § 102. *Net MoneyIN*, 545 F.3d at 1371 (emphasis added) (quoting *Arkley*, 455 F.2d at 587). Thus, the rejections should be withdrawn even if *H.225*, *H.235*, and *H.245* are incorrectly incorporated by reference into *H.323*.

1. Independent Claim 1

a. The Combined *H.323* References Do Not Disclose "a First Device Associated with a Secure Name and an Unsecured Name"

In its prior Response, Patent Owner comprehensively traversed the Office's various arguments regarding the "secure name" and "unsecured name" recited in claim 1. (Response at 54-55; Req. at 208-13; OA at 11-12, incorporating Request by reference.) The Office did not rebut any of Patent Owner's arguments, and Requester only reasserted two of its prior arguments, one regarding access tokens and the other relating to the URL of a gatekeeper, alleged to correspond to an "unsecured address." (Second OA at 80; Comments at 30.)

Rather than maintain its prior arguments for the rejection, the Office instead proposed a new one: that a "name and address . . . linked via a registry" correspond to the secure name and unsecured name recited in claim 1. (Second OA at 80.) The Office explains that the alleged secure name is a "generic name . . . such as a phone number or email address," while "the address itself (capable of accessing the network end), is an unsecure means of access." (*Id.*) The Office's new rejection is incorrect and should be withdrawn. In the alternative, a non-final office action should issue because the issues in this proceeding remain far from clear, given the altered positions newly taken by the Office regarding the "secure name" and "unsecured name" of claim 1. M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed.").

First, the Office is incorrect that a "generic name . . . such as a phone number or email address" corresponds to the "secure name" recited in claim 1. The Office offers no support for its assertion, (*see* Second OA at 80), and claim 1 recites a "secure name," not a "generic name," so the new rejection has no bearing on the claim language. To the extent that the Office relies on

Requester's claim construction arguments advocating that "secure name" and "unsecured name" should be construed solely by referring to the '181 patent prosecution history and to a prior reexamination of the '180 patent, the Office is mistaken for the reasons discussed above in Section V.A.1.a.i. M.P.E.P. § 2258(I)(G).

The Office is also incorrect that an address "capable of accessing the network end" (i.e., a network address) corresponds to an "unsecured name." (*See* Second OA at 80.) Claim 1 recites two separate names—a "secure name" and an "unsecured name"—as well as "a network address corresponding to the secure name." The Office attempts to conflate the "unsecured name" and "network address" claim terms. As a result, the Office's rejection is based upon an arrangement of *H.323* features in which only two of the three recited claim features ("secure name," "unsecured name," and "network address corresponding to the secure name") could possibly be present.

For all of the above reasons, the incorrectly combined *H.323* references do not disclose "a first device associated with a secure name and an unsecured name," and the rejection of claim 1 should be withdrawn.

b. The Combined *H.323* References Do Not Disclose "Receiving, at a Network Address Corresponding to the Secure Name Associated with the First Device, a Message from a Second Device of the Desire[] to Securely Communicate with the First Device"

As with the "secure name" and "unsecured name" features, Patent Owner comprehensively traversed the Office's various arguments regarding the claim 1 features of "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." (Response at 56-58.) The Office maintained the rejections based on the token embodiments of *H.323* and *H.235*, and the IPSEC embodiment of *H.235*. (Second OA at 80-83.) The rejections should be withdrawn for the reasons discussed below and in Patent Owner's previous Response. (Response at 56-58.)

(i) The Office's Token-Based Arguments Are Incorrect

The Office argues that a mere "request to communicate" in the token embodiments discloses these claim features. (Second OA at 81.) But the Office's arguments do not account for the specific recitations in claim 1, i.e., that the alleged "message" of claim 1—the Office's "request to communicate"—is modified by the phrase "of the desire[] to securely communicate," and that the recited "message" must also come from the "second device" and be "receiv[ed], at a network address corresponding to the secure name associated with the first device." The Office has yet to identify any particular alleged "request to communicate" in the token embodiments that is "of the desire[] to securely communicate." (*Id.* at 80-83; Req. at 214-15.) Accordingly, the rejection should be withdrawn.

The Office alleges that an endpoint having a token-protected alias address corresponds to the "first device associated with a secure name" of claim 1. (Req. at 213.) But in the token embodiments, the alleged "second device" does not perform any functions that correspond to the features assigned to it in the claim. (Supp. Keromytis Decl. ¶ 15.) For example, in the "security token" embodiment of *H.235*, Endpoint A (the alleged second device) initially sends a regular ARQ message to its gatekeeper to resolve the address of the gateway. (*H.235* 28.) In the ACF message, the gatekeeper then returns the gateway's address and the security token containing the E.164 phone number of POTS-B (the alleged first device). (*Id.*) Next, Endpoint A sends a SETUP message to the gateway with the security token, and the gateway sends the security token back to the gatekeeper for deciphering. (*Id.* at 28-29.) This ends *H.235*'s disclosure. (*See id.*) None of these messages is sent *from* the alleged second device (Endpoint A) and "receiv[ed], at a network address corresponding to the secure name associated with" the alleged first device (POTS-B). (Supp. Keromytis Decl. ¶ 16.) Rather, POTS-B does not receive any message at all in the disclosure of *H.235*, let alone a "message . . . of the desire[] to securely communicate" from Endpoint A. (*Id.*)

The Office's alleged "request to communicate" sent by a calling endpoint (i.e., the alleged second device) in these embodiments further does not correspond to a "message . . . of the desire[] to securely communicate." In the token embodiments, the calling endpoint never sends a request to communicate, desiring the use of a protective token to a called endpoint. Rather, the tokens are wielded by the called endpoint (i.e., the alleged first device) and used in combination with a gatekeeper so that a calling endpoint cannot obtain the called endpoint's transport address and communicate directly with the called endpoint. (*Id.* ¶ 17.) Indeed, *H.323* describes its tokens as "provid[ing] privacy by shielding an endpoint's Transport Address and Alias address information *from a calling party*." (*H.323* 38, emphasis added; *see also H.235* 28, "Assume that EPA [Endpoint A] is trying to call POTS-B, *and POTS-B does not want to expose its E.164 phone number to EPA*," emphasis added.) Called endpoints simply register their tokens with their gatekeepers and use the gatekeepers to shield them from calling endpoints. (*H.235* 28-29; *H.323* 38.)

The rejection should also be withdrawn because the Office's maintained rejection relies on multiple features as corresponding to the "secure name" of claim 1. As discussed above, the Office argues that the "secure name" of claim 1 corresponds to a "generic name . . . such as a phone number or email address," while "the address itself (capable of accessing the network end), is an unsecure means of access." (*See supra* Section VII.B.1.a; Second OA at 80.) The Office did so despite Requester urging the Office to maintain a token-based rationale for the rejection. (Second OA at 80.) Yet when addressing the claim feature of "receiving, at a network address corresponding to the *secure name* associated with the first device, a message from a second device of the desire[] to securely communicate with the first device" (emphasis added), the Office now argues that a token provides "the secure naming structure." (*Id.* at 81.) Thus, for the preamble of claim 1, the Office relies upon a "generic name" as corresponding to the "secure name," while relying on an access token or security tokens for the "secure name" for the "receiving, at a network address . . ." feature of claim 1. Because the Office is inappropriately mixing and matching different portions of the combined references as corresponding to the "secure name" for the different elements of claim 1, the rejection should be withdrawn. *Therasense*, 593 F.3d at 1332 ("[C]laims cannot be 'treated . . . as mere catalogs of separate parts, in disregard to the part-to-part relationships set forth in the claims and that give the claims their meaning.'" (citation omitted)).

For all of the reasons set forth above, as well as those in Patent Owner's previous Response, the token-based rejections of claim 1 should be withdrawn. (Response at 56-58.)

(ii) The Office's IPSEC-Based Rejections Are Incorrect

The Office and Requester disregard the claim language in asserting that the IPSEC feature of *H.235* discloses the above-referenced feature of claim 1. Whereas claim 1 specifically recites "a message from a second device of the desire[] to securely communicate" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device," the Office and Requester incorrectly focus on broad descriptions of "negotiations" between endpoints, such as a request for session initiation "followed then either by an accepted or rejected decision by the other network end." (Second OA at 82-83.) This overbroad and unreasonable analysis overlooks the specific "message" recited in the claim and the various specific claim features related to this "message." A proper analysis reveals that not a single message or step within these "negotiations" in the cited passages of *H.323* and *H.235* corresponds to "a message from a second device of the desire[] to securely communicate" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device."

The Office and Requester rely on the *H.235* IPSEC feature involving an endpoint and a gatekeeper. (Req. at 215-16, quoting *H.235* at 30-31.) Requester asserts that in this IPSEC feature, "the endpoints can negotiate the use of IPSEC for the H.245 channel" during the SETUP and CONNECT exchange in establishing an *H.245* control channel. (Second OA at 82.) Requester contends that this SETUP and CONNECT exchange, mediated by at least one gatekeeper facilitating "routed call signaling," discloses the claim features of "a message from a second device of the desire[] to securely communicate" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device," and can be shown in Figure 23 of *H.323*, reproduced below:

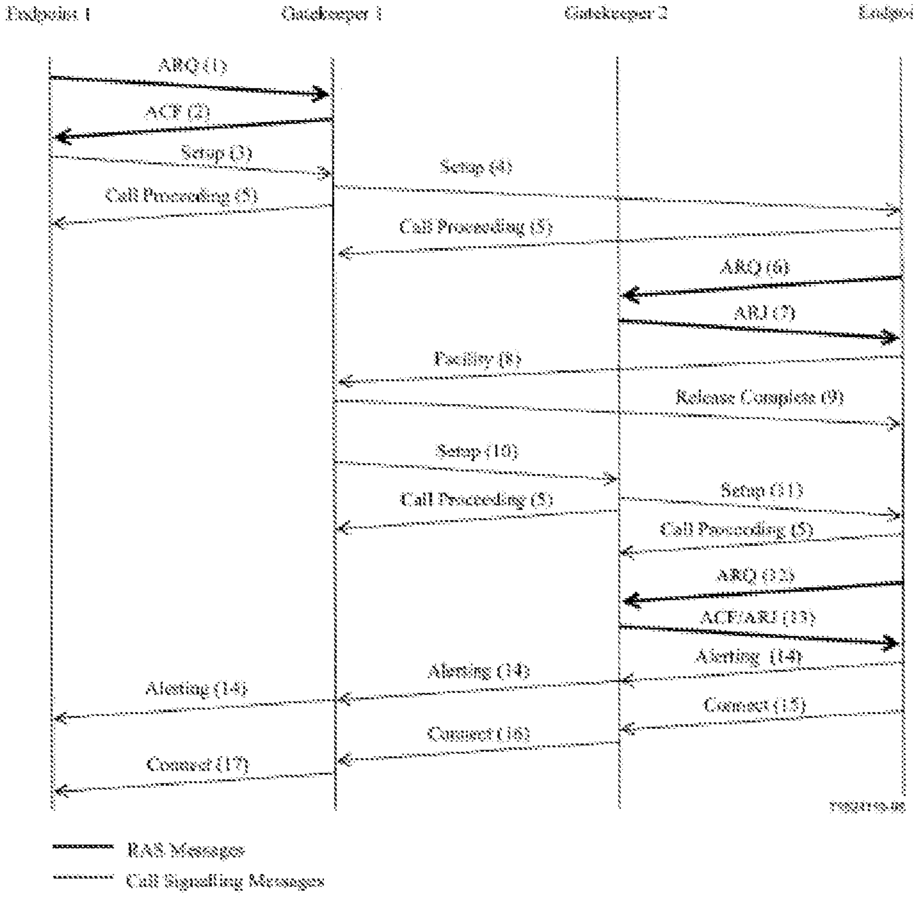


Figure 23/H.323 – Both endpoints registered – Both Gatekeepers routing call signalling

(*H.323* at 51, Fig. 23, showing setup and connection of an *H.245* control channel.)

At least sixteen of the seventeen different messages shown and described in Figure 23, however, are either sent from an endpoint to a gatekeeper, or from a gatekeeper to an endpoint—not from the alleged second device to the first device, as required by the claim. (*Id.* at Fig. 23; *cf.* "Alerting (14)"; Supp. Keromytis Decl. ¶ 20.) Indeed, *H.323* specifies that for Requester's alleged SETUP exchange, "Gatekeeper 1 shall return a Call Signalling Channel Transport Address of itself in the ACF (2) [to Endpoint 1]. *Endpoint 1 then sends the Setup (3) message using that Transport Address*." (*H.323* 50, emphasis added.) As a result, the Setup (3) message is sent from Endpoint 1 to

Gatekeeper 1, and accordingly cannot correspond to the claim 1 feature of "a message from a second device" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device."

The Setup (4) message also cannot correspond to the recited feature of claim 1. (*Id.* at 51, Fig. 23; Supp. Keromytis Decl. ¶ 21.) With respect to Figure 23, *H.323* specifies that "Gatekeeper 1 then sends the Setup (4) message to the well-known Call Signalling Channel Transport Address of Endpoint 2." (*H.323* 50.) Thus, the Setup (4) message is sent from Gatekeeper 1 to Endpoint 2, and also cannot correspond to the claim 1 feature of "a message from a second device" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device." The other messages cited by Requester, such as the ARQ(6) and ACF(7) messages, are also only sent between an endpoint and a gatekeeper. (*H.323* 51, Fig. 23.) Accordingly, none of the messages within the "SETUP and EXCHANGE" exchange during the setup of an IPSEC-protected *H.245* control channel disclose the claim feature. (*Id.* at 50-51; *H.235* 30-31.) As a result, the rejections should be withdrawn.

The Office, meanwhile, further asserts that a "request for the session initiation . . . followed then either by an accepted or rejected decision by the other network end" corresponds to "a message from a second device" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device," as recited in claim 1. The Office is incorrect. As shown in Figure 23 and described in the accompanying text, the Endpoint 1 initiates a session by interacting exclusively with Gatekeeper 1 during the "ARQ (1)/ACF (2) exchange." (*H.323* 50-51.) Then, for the accept/reject decision, "[i]f Endpoint 2 wishes to accept the call, it initiates the ARQ(6)/ACF(7) exchange with Gatekeeper 2," illustrating that this process is similarly nothing more than an exchange of messages between Endpoint 2 and Gatekeeper 2. (*Id.*; Supp. Keromytis Decl. ¶ 22.) Thus, the "request for the session initiation" and the "accepted or rejected decision" relied upon by the Office fails to disclose the claim features.

Both the Office and Requester have failed to identify a single message corresponding to the claim 1 feature of "a message from a second device of the desire[] to securely communicate" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device." The rejections should be withdrawn.

c. The Combined *H.323* References Do Not Disclose "Sending a Message over a Secure Communication Link from the First Device to the Second Device"

The Office dismissed Patent Owner's arguments by asserting that "Patent Owner 'raises no new arguments' in response to the above claim limitation." (Second OA at 83-84.) However, Patent Owner did raise distinct arguments, and the Office incorrectly maintained the rejection over Patent Owner's unaddressed arguments.

In its previous Response, Patent Owner explained that the Office had not identified any feature within the combined *H.323* references that allegedly corresponds to "sending a message over a secure communication link from the first device to the second device." (*Id.*) The Office still has yet to identify this feature from the combined *H.323* references, or otherwise assert that this feature is somehow inherent. (*See id.* at 84.) For this reason, as well as for the others asserted in Patent Owner's previous Response, the rejection of claim 1 is deficient and should be withdrawn. *Net MoneyIN*, 545 F.3d at 1369 ("[T]he proponent must show 'that the four corners of a single, prior art document describe every element of the claimed invention.'" (citation omitted)); (Response at 58-59).

2. Independent Claim 2

a. The Combined *H.323* References Do Not Disclose "a Secure Name"

The Office raises no additional arguments regarding the "secure name" beyond those argued with respect to claim 1. (Second OA at 84; *id.* at 80.) Accordingly, the Office's rejection is deficient and should be withdrawn for similar reasons to those discussed above with respect to claim 1.

b. The Combined *H.323* References Do Not Disclose "a Network Address Associated with the Secure Name of the Second Device"

The Office and Requester rely on the IPSEC feature of *H.235* to show "a network address associated with the secure name of the second device." (*Id.* at 84-85.) This is incorrect.

The only address relied upon in the quoted passage of *H.323* is a "well-known" transport address relating to a call signalling channel of Endpoint 2. (*H.323* 50, "well-known Call Signalling Channel Transport Address.") A "transport address" is nothing more than a basic network address with a TSAP identifier. (*Id.* at 8, defining "transport address.") *H.323* does not associate the well-known call signalling channel transport address with any name of an endpoint at all, let alone a "secure name." (*Id.* at 50.) It is not associated with any particular "secure name," given that *H.323* describes it as "well-known." (*Id.*; Supp. Keromytis Decl. ¶ 24.) Moreover, the Office argued with respect to claim 1 that the network address itself (e.g., a "transport address") corresponds to an "unsecured name." (Second OA at 80; *see also supra* Section VII.B.1.a.) Thus, the rejection should be withdrawn because the transport address highlighted by the Office as corresponding to the "network address" of claim 2 is not "associated with the secure name of the second device," as recited in the claim.

c. The Combined *H.323* References Do Not Disclose "from the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated with the Secure Name of the Second Device" and "at the First Device, Receiving a Message Containing the Network Address Associated with the Secure Name of the Second Device"

As discussed above, the Office relies on the IPSEC embodiment of *H.235* to allegedly show "a network address associated with the secure name of the second device," as recited in claim 2. This embodiment involves no "message requesting a network address" or network address resolution, however, since the transport address utilized is already "well-known." (*H.323* 50.) Thus, to allege disclosure of these claim features, and particularly the feature of "sending a message to a secure name service, the message requesting a network address," the Office switches to the "security token" embodiment. (Second OA at 85-87, citing *H.235* 28.) By relying on one embodiment involving network address resolution for certain features, and another embodiment not involving any network address resolution for other features, the Office has incorrectly picked and chosen different features from different, inconsistent embodiments, and the rejection of claim 2 should be withdrawn. *Net MoneyIN*, 545 F.3d at 1370 (anticipation requires that a reference "show all of the limitations of the claims *arranged or combined in the same way as recited in the claims*" (emphasis added)).

Moreover, the Office's security-token arguments are incorrect and fail to anticipate the claim for the reasons discussed below.

(i) The Security Token Embodiment Does Not Disclose "from the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated with the Secure Name of the Second Device"

The security token embodiment fails to disclose "from the first device, sending a message to a secure name service, the message *requesting a network address associated with the secure name* of the second device" (emphasis added). As discussed above, the Office argues that a "generic name," such as phone number or email address, corresponds to a "secure name." (Second OA at 80, 84.)

Within the security token embodiment, POTS-B allegedly corresponds to the "second device" while Endpoint A allegedly corresponds to the "first device." (Req. at 221.)

In this embodiment, however, Endpoint A cannot send any alleged "message requesting a network address *associated with the secure name* of the second device" (emphasis added) because POTS-B has shielded its alleged "secure name"—the E.164 phone number—from Endpoint A with the security token. (*H.323* 28; Supp. Keromytis Decl. ¶ 25.) *H.325* explains that security tokens act to "obscure or hide destination addressing information." (*H.325* 28) Indeed, the POTS-B device wields a security token because "POTS-B does not want to expose its E.164 phone number to [calling Endpoint A]." (*Id.*) Thus, rather than requesting a name associated with POTS-B's E.164 phone number—which, of course, it cannot do—Endpoint A instead sends an ARQ to the gatekeeper to resolve the address of the Gateway between POTS-B and Endpoint A. (*H.235* 28, the address "*as represented by its alias/GW*," emphasis added.)

Because the security token embodiment fails to disclose at least the claim feature of a "message requesting a network address *associated with the secure name* of the second device" (emphasis added), the rejection of claim 2 should be withdrawn.

(ii) The Security Token Embodiment Does Not Disclose "at the First Device, Receiving a Message Containing the Network Address Associated with the Secure Name of the Second Device"

Just as the security token embodiment fails to disclose "sending a message *requesting* a network address associated with the secure name of the second device," it also fails to disclose "receiving . . . a message *containing* the network address associated with the secure name of the second device" (emphases added). The Office argues that "returning the address of the gateway associated with the second device is sufficient to read on the claim." (Second OA at 86.) The Office is incorrect.

The plain language of the claim recites that the network address received is "associated with the secure name of the second device." But the Office's argument incorrectly incorporates a third device into the claim, as shown below with the Endpoint A (alleged first device), POTS-B (alleged second device), and the third device: the Gateway.

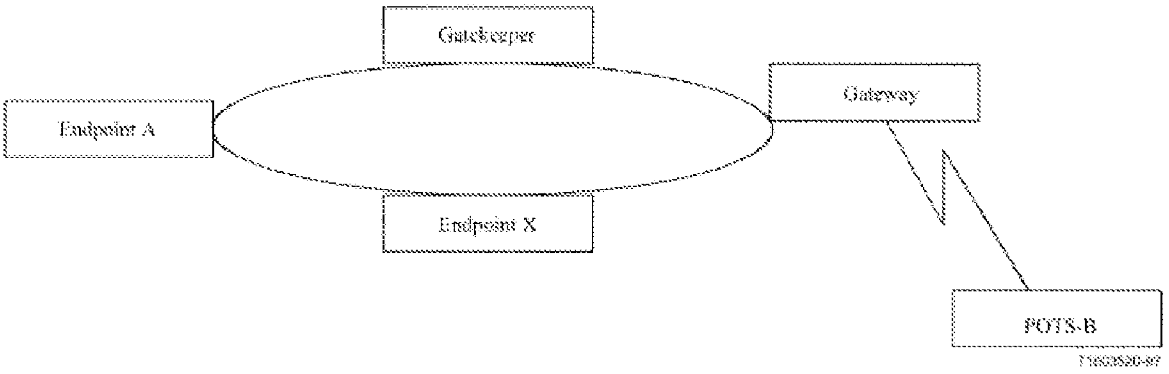


Figure I.6/H.235

(*H.235* 28, Fig. I.6.) Thus, the Office attempts to rewrite the claim to recite "receiving a message containing the *network address associated with a third device* (gateway) *that can communicate with the second device*." Nowhere do the Office nor Requester attempt to justify their dramatic expansion of the plain claim language, instead concluding without any analysis that a feature meeting their dramatic expansion "is sufficient to read on the claim." (Second OA at 86.)

The Office and Requester are incorrect. They claim without any support that any limitations on the claim term "associated" are simply "non-existent." (*Id.*) This analysis contravenes Federal Circuit law. *See, e.g.*, *In re Abbott*, 696 F.3d at 1148. Any broadest reasonable interpretation of the claims must be "consistent with the specification," whereas the Office does not attempt to find any support in the specification when effectively reading "associated" out of the claim language. *Id.*; M.P.E.P. § 2258(I)(G).

Moreover, anticipation law requires that a reference must precisely "disclose[] within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim." *Net MoneyIN*, 545 F.3d at 1371. The Office's conclusory pronouncement that a third device can be added and is "sufficient to read on the claim," without any consideration of the actual claim language, fails to support the rejection. The rejection should be withdrawn.

d. The Combined *H.323* References Do Not Disclose "from the First Device, Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

Having relied on the security token embodiment of *H.235* for the "sending a message . . . requesting the network address . . ." and "receiving a message containing the network address . . . ," the Office switches back again to the IPSEC embodiment of *H.235* for the feature of "sending a message to the network address associated with the secure name of the second device using a secure communication link." (Req. at 224-26, relying on the IPSEC embodiment; Second OA at 88, presenting no other substantive arguments.) These embodiments are inconsistent for at least the reasons discussed above, and, accordingly, the Office's rejection is predicated on incorrect picking and choosing from among multiple inconsistent embodiments for each different feature of claim 2. *Net MoneyIN*, 545 F.3d at 1371.

Thus, the rejections should be withdrawn for the reasons stated above, as well as those in Patent Owner's previous Response. (Response at 62.)

3. Dependent Claims 3-23

Claims 3-23 depend directly or indirectly from claim 2 and are patentable for at least the reasons discussed above with respect to claim 2 and in Patent Owner's previous Response. (*Id.* at 59-64.) In addition, the rejections of claims 4, 5, 9-11, 13, and 21 should be withdrawn for the reasons set forth below.

4. Dependent Claim 4

After having relied on an alias address in the "security token" embodiment of *H.235* as disclosing the features of claim 4 in its original Request, Requester now takes the new position in its Comments that an *H.323* access token "indicate[s] security," and therefore discloses that "the secure name indicates security," as recited in claim 4. (Second OA at 87, quoting Comments at 34-35; Req. at 227.)

In its analysis, however, Requester completely ignores the claim language specifying that the "secure name" itself indicates security. As *H.323* explains, an access token merely shields an endpoint's alias address or transport address. (*H.323* 38.) At no point does *H.323* describe an access token *itself* as any type of name or address, and nor does Requester assert that it does. Requester's analysis is irrelevant to the actual claim language, so the rejection should be withdrawn. In the alternative, the Office should reopen prosecution since Patent Owner has not yet had an opportunity in a non-final office action to respond to the new rejection predicated on the "access token" of *H.323*. M.P.E.P. § 2673.01(I) ("The patent owner *must* be given an opportunity to adequately address any change in position adverse to the patent owner's position." (emphasis added)).

The Office, meanwhile, argues that a "generic name," such as a phone number or an email address, corresponds to a secure name. (Second OA at 80.) The Office does not assert that a phone number or email address "indicates security," as recited in claim 4, nor does it explain how any other feature might correspond to indicating security. Rather, the Office merely expresses agreement with Requester's access-token argument by stating that with the access token, "these are levels of security, where each of the references desire for layers of securing information show a layering of hidden addresses, encryption, and other means of securing network communications." (*Id.*) This argument is incorrect for the reasons stated above, and the Office's further argument about various "means of securing network communications" has no bearing on the claim feature providing that "the secure name indicates security."

By persisting with arguments about features outside of the *H.323* naming scheme, the Office fails to identify any secure name that "indicates security." Thus, the rejection of claim 4 should be withdrawn for the reasons stated above and in Patent Owner's previous Response. (Response at 63.) In the alternative, prosecution should be reopened because the Office has adopted a new basis for the rejection, as discussed above. M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed.").

5. Dependent Claim 5

Requester and the Office incorrectly dismiss Patent Owner's arguments regarding claim 5. The Office asserts that Patent Owner's arguments are not distinct from its arguments regarding claim 2 and therefore do not merit a reply because the Office already addressed those arguments. (Second OA at 89.) However, for the relevant "receiving a message . . ." feature of claims 2 and 5, the Office's arguments in the Second Office Action only addressed the "security token" and "access token" embodiments, whereas the maintained rejection of claim 5 relied exclusively upon the IPSEC feature of *H.235*. (*Id.* at 86-87; Req. at 227-28.) The Office did not address any of Patent Owner's arguments with respect to the IPSEC embodiment for the "receiving a message . . ." feature of claim 2. (Second OA at 86-87; *see* Response at 61-62.) Neither did Requester. (Comments at 33-34.) Thus, the Office dismisses Patent Owner's arguments as unpersuasive while purporting to have already addressed them, but the Office in fact never addressed those arguments. Rather, it abandoned its earlier position regarding the IPSEC embodiment with respect to the "receiving a message . . ." feature of claim 2 in the Second Office Action. (*Compare* Second OA at 86-87; Comments at 33-34 *with* Req. at 222-24.)

Because the Office no longer relies on the IPSEC embodiment of *H.235* after Patent Owner's previous Response regarding the feature of "receiving a message . . ." recited in claims 2 and 5, the rejection of claim 5—predicated exclusively on this same IPSEC embodiment—should be withdrawn.

Moreover, it is incorrect for the Office to adopt a rejection, dismiss Patent Owner's arguments as previously addressed when in fact they were not addressed, and then maintain the rejection and close prosecution. An ACP is only permitted "[u]pon consideration of the issues a second or subsequent time." 37 C.F.R. § 1.949; *see also* M.P.E.P. § 2671.02. Because Patent Owner has yet to be heard regarding its Response to the rejection of claim 5 in the First Office Action, prosecution should be reopened. Moreover, the rejection should be withdrawn for the reasons stated above and in Patent Owner's previous Response. (*See* Response at 63.)

6. Dependent Claim 9

The Office and Requester do not show how the combined *H.323* references disclose "automatically initiating the secure communication link after it is enabled." (Second OA at 89.) Requester argues that the mere feature of "dynamically" updating an endpoint's security policy within the IPSEC embodiment corresponds to these claim features. (*Id.*) But at that point in the IPSEC embodiment, no secure communication link is being initiated, let alone already been "enabled," as recited within the claim. (Supp. Keromytis Decl. ¶ 26.) *H.235* explains that the endpoints continue to have significant non-automatic authentication hurdles before any IPSEC-protected communications are enabled or subsequently initiated. (*H.235* 30.) For example, *H.235* specifies that "person-to-person Q&A" and "user-to-user authentication" are involved in negotiating the characteristics of the channel "before any H.245 packets are transmitted." (*Id.*) The Office does not supplement Requester's deficient argument, and, accordingly, the rejection should be withdrawn.

7. Dependent Claims 10 and 11

As discussed above in Section VII.B.2.c, the combined *H.323* references do not disclose "receiving a message containing the network address associated with the secure name," as recited in claim 2, let alone receiving such a message "through tunneling" or "in the form of at least one tunneled packet," as recited in claims 10 and 11, respectively. Thus, the rejection of claims 10 and 11 should be withdrawn.

Moreover, Requester is incorrect in asserting that merely because *H.245* messages generally "can be encapsulated in any Q.931 message," this means that the specific claimed message "containing a network address associated with the (alleged) secure name" is encapsulated in this manner. (Comments at 35-36, arguing that a "SETUP" message discloses the "message" recited in the claims.) Rather, as *H.323* describes with respect to Figure 23, specifically relied upon by Requester earlier, the SETUP (3) and SETUP (4) messages involve no message containing any network address, let alone one "associated with the secure name." (*H.323* 50-51, instead utilizing "well-known" transport addresses.) The Office does not remedy Requester's arguments, and its broad assertion that "H.245 messages are capable of being encapsulated" entirely disregards the specific "message containing the network address" feature recited in claims 10 and 11. As a result, the rejection should be withdrawn.

8. Dependent Claim 13

Claim 13 incorporates the features of claim 2, "wherein the receiving and sending of messages through the secure communication link includes multiple sessions." Patent Owner previously rebutted this rejection by arguing that the feature relied upon by the Office would require setting up separate logical channels, which is inconsistent with the singular "secure communication link" recited in the claim. (Response at 64.) Having previously relied upon a single H.245 channel within the IPSEC embodiment as corresponding to the "secure communication link" of claim 2, Requester now dramatically expands its interpretation of "secure communication link" to include many such channels. (Second OA at 91-92.) Nowhere does Requester attempt to justify its dramatic expansion of the plain claim language, instead claiming that any limitations on the *singular* claim term "secure communication link" are "non-existent." (*Id.*) Any broadest reasonable interpretation of the claims must be "consistent with the specification," but Requester does not attempt to find support in the specification for its interpretation contrary to the actual claim language. *Abbott*, 696 F.3d at 1148; M.P.E.P. § 2258(I)(G). Because the Office's rejection depends on Requester's deficient arguments, the rejections should be withdrawn for the reasons discussed above and in Patent Owner's previous Response. (Response at 64.)

9. Dependent Claim 21

In light of the Office's new arguments regarding the "secure name" and "unsecured name" discussed above with respect to claim 1, the rejection of claim 21 should be withdrawn for the same reasons discussed above for claim 1.

10. Independent Claim 26 and Dependent Claim 27

The Office dismisses Patent Owner's arguments as allegedly "present[ing] no response that is distinct from those answered above." (Second OA at 92.) The Office is incorrect. As explained in Patent Owner's previous Response, the Office has not shown how *H.323* allegedly discloses "an unsecured name associated with the first device" and a "*unique network address* correspond[ing] to the secure name associated with the first device." (Response at 65.) The Office did not address these features in any previous part of its *H.323* section in the Second Office Action. Thus, the rejection should be withdrawn for the unrebutted reasons stated in Patent Owner's previous Response. (*Id.*)

Moreover, it is incorrect for the Office to adopt a rejection, dismiss Patent Owner's arguments as previously addressed when in fact they were not addressed, and then maintain the rejection and close prosecution. An ACP is only permitted "[u]pon consideration of the issues a second or subsequent time." 37 C.F.R. § 1.949; *see also* M.P.E.P. § 2671.02. Prosecution should be reopened because Patent Owner's arguments have not yet been considered, and the rejection should be withdrawn for the reasons stated above and in Patent Owner's previous Response. (Response at 65.)

11. Independent Claims 24 and 28 and Dependent Claims 25 and 29

Although of different scope, claims 24, 25, 28, and 29 include recite features similar to the features of independent claims 1 and 2, as discussed in Patent Owner's previous Response. (*Id.* at 64-66.) Thus, for reasons similar to those discussed above for claims 1 and 2, and for the reasons set forth in Patent Owner's previous Response, the rejections should be withdrawn. (*Id.*)

IX. The Rejection of Claims 1-16 and 18-29 Based on *Johnson* in View of RFC 2131, RFC 1034, and RFC 2401 Should Be Withdrawn (Issue 13)

The Second Office Action rejects claims 1-16 and 18-29 under 35 U.S.C. § 103(a) based on *Johnson* in view of RFC 2131, RFC 1034, and RFC 2401. (Second OA at 12.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

A. Independent Claim 1

1. *Johnson*, Either Alone or in Combination with RFC 2131, RFC 1034, and RFC 2401, Does Not Disclose "a First Device Associated with a Secure Name and an Unsecured Name"

Requester contends that the name of the secure mail server registered by the secure name service corresponds to the recited "secure name." (Comments at 37-39.) Meanwhile, Requester argues that three separate things correspond to the claimed "unsecured name": (1) the name of the secure name server allegedly registered with a DHCP; (2) the domain names of the secure name server and secure mail server allegedly registered in the public DNS system; and (3) the alleged "client identifiers" associated with the domain names of the secure name server and secure mail server. (*Id.*) The Office appears to agree and further contends, for the first time, that the dynamic address associated with the secure mail server also corresponds to the claimed "unsecured name." (Second OA at 96-98.) These rejections should be withdrawn at least because the name of the secure mail server does not disclose the claimed "secure name" under either a proper construction of the term or Requester's own flawed construction, and because RFC 2131 and RFC 1034 fail to cure the deficiencies of *Johnson* with respect to the "unsecured name" recited in claim 1.

a. *Johnson* Does Not Disclose a "Secure Name"

Requester and the Office advance two constructions for the term "secure name." (Comments at 37-38; Second OA at 94-96.) The first relies on out-of-context external statements while failing to consider the '181 patent specification itself. (Comments at 37-38; Second OA at 94-95.) The second is Requester's own construction, adopted by the Office. (Comments at 37-38; Second OA at 95-96.)

A proper analysis discloses that the secure mail server's name does not satisfy either of these flawed constructions.

Requester's and the Office's first construction of "secure name" relies solely on statements from the '181 patent prosecution history and a reexamination of the related '180 patent. (Comments at 37-38; Second OA at 94-95.) As discussed above in Section V.A.1.i, such a construction, ignoring the specification, is incorrect. *See* M.P.E.P. § 2258(I)(G).

Patent Owner does not dispute that the term "secure name" refers to those names used to communicate securely that are resolved by a secure name service, consistent with its statements during prosecution. However, Patent Owner does not agree with Requester's and Office's contentions that the secure name service is nothing more than that. (Comments at 37-38; Second OA at 94-95.) Not only do the embodiments described in the '181 patent specification explain that the secure name service must do more, but the Office relies on statements in the '180 patent reexamination that refer to just such an embodiment. (*See* Order at 5, citing '180 patent 51:25-35, corresponding to '181 patent 50:15-25.) As described in more detail above in Section V.A.1.i, this embodiment of the '181 patent specification explains that "SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link." ('181 patent 51:15-17.) Accordingly, the secure name service must not only resolve secure names, but further support establishing a secure communication link. (Keromytis Decl. ¶ 121.) The secure name service of *Johnson* fails to provide such support, and the Office and Requester do not dispute this. (*See* Second OA at 94-95; Comments at 37-38.) Because the secure name service of *Johnson* does not further support establishing a secure communication link, the name of the secure mail server cannot correspond to the "secure name" as claimed.

Requester and the Office next assert that a "secure name" is one that "requires authorization to access and is protected through encryption." (Req. at 272; First OA at 12.) However, when Patent Owner analyzes the secure mail server's name with respect to this construction, Requester and the Office protest that the Owner is reading non-existent claim limitations into the claim. (Comments at 38; Second OA at 95-96.) Patent Owner does no such thing. As discussed in detail in Patent Owner's previous Response, *Johnson* does not teach or suggest that the name of the secure mail server requires authorization to access or that it is protected through encryption. (Response at 68.) Instead, *Johnson* teaches that the user knows the name of the secure mail server, but never discusses whether the user required authorization to access the name or whether the name was protected through encryption during access. (*See, e.g.*, *Johnson* 7:12-17, 9:25-27; Keromytis Decl. ¶ 122.) Requester and Office do not contest this fact. This is not a non-existent claim limitation read into the claim by Patent Owner, but a necessary consequence of Requester's own proposed construction. Given that Requester has asserted that a secure name "requires authorization to access and is protected through encryption," it is only expected that the name Requester relies upon should satisfy both of these criteria. The name of the secure mail server does neither.

In view of the above, and because neither Requester nor the Office relies on any of RFC 2131, RFC 1034, and RFC 2401 for the "secure name," *Johnson* does not disclose that claim feature either alone or in view of RFC 2131, RFC 1034, and RFC 2401.

b. *Johnson*, Either Alone or in Combination with RFC 2131 and RFC 1034, Does Not Disclose an "Unsecured Name"

In the First Office Action, the Office conceded that *Johnson* did not disclose the claimed "unsecured name," and looked to *Johnson* in combination with either RFC 2131 or RFC 1034 to meet the claims. (First OA at 12, incorporating by reference the Request at 270-318.) But in an about-face, the Office now additionally contends that the dynamic address of the secure mail server in *Johnson* alone corresponds to the "unsecured name." The Office is incorrect. Moreover, because *Johnson* teaches away from the address allocation and registration of RFC 2131 and because one of ordinary skill in the art would not have been motivated to combine the secure communication system of *Johnson* with the open-access DNS system of RFC 1034, *Johnson* in view of RFC 2131 and RFC 1034 also does not disclose the claimed "unsecured name."

Contrary to the Office's contentions, the dynamic address of the secure mail server does not correspond to the claimed "unsecured name." As *Johnson* explains, the dynamic address is an "Internet protocol address" and not a "name" at all. (*Johnson* 6:27-29.) Further, the Office and Requester both admit that "the dynamic address of the secure electronic mail server 16 is not easily obtained." (Req. at 272, citing *Johnson* 8:2-3; First OA at 12, incorporating by reference the Request at 270-318.) For example, *Johnson* discloses that "because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server." (*Johnson* 8:4-8.) In addition, a user must be authorized by the secure name server in accordance with a unique logon protocol simply to access the server at all. (*Id.* at 7:12-14.) As a result, the dynamic address of the secure mail server fails to correspond to the claimed "unsecured name." Moreover, because an ACP is not permitted to raise new grounds for rejection, prosecution should be reopened and the rejection withdrawn at least for the reasons discussed here. *See* 37 C.F.R. § 1.949; *see also* M.P.E.P. § 2671.02.

Attempting to meet the claim term, the Office next turns to a combination of *Johnson* with RFC 2131. Requester contends, and the Office agrees, that the secure mail server's dynamic address would be allocated in accordance with the Dynamic Host Configuration Protocol (DHCP) discussed in RFC 2131. (Req. at 272-73; First OA at 12.) However, *Johnson* teaches away from using the Dynamic Host Configuration Protocol of RFC 2131. RFC 2131 teaches the following:

> DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "manual allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client.

(RFC 2131 2.) *Johnson* does not rely on any of these methods to assign a dynamic address to the secure mail server. According to *Johnson*, "the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network." (*Johnson* 6:26-27.) Unlike the "manual allocation" defined in RFC 2131, *Johnson* identifies no DHCP server to convey the address to the secure mail server from the network. Even assuming such a DHCP server was used to convey the information in *Johnson*, RFC 2131 explains that only "dynamic allocation" allows for the assignment of dynamic addresses. Thus, even if the secure mail server were modified to receive an address in accordance with the "manual allocation" taught in RFC 2131, that address would be fixed—not the dynamic address taught in *Johnson*. Requester further asserts that in accordance with RFC 2131, the secure name server would register with a DHCP server and receive a client identifier that satisfies the claimed "unsecured name." (Req. at 273-74.) However, *Johnson* again teaches away from RFC 2131, describing only that the secure mail server registers with a secure name service and does not receive anything in response. As a result, one of ordinary skill in the art would not have looked to combine *Johnson* with RFC 2131.

Requester and the Office also contend that because both *Johnson* and RFC 1034 attempt to solve the problem of "improving access of interbusiness communications," one of ordinary skill in the art would modify the secure name server and secure mail server of *Johnson* such that they would register domain names in the public DNS. (Req. at 274; First OA at 12, incorporating by reference the Request at 270-318.) But the problems and solutions proposed by *Johnson* and RFC 1034 are diametrically opposed. While *Johnson* is concerned with security and the prevention of public access to communications across network systems, (*Johnson* 1:20-28), Requester admits that RFC 1034 is directed to improving and expanding public access to communications using a user-friendly naming scheme, (Comments at 40). Discussing security, *Johnson* explains that "the remote administrator 20 will establish logon protocol for users to access the secure name server 14," which it will pass on to users of the protected communication network such that "only users authorized by the remote administrator 20 will be allowed to access the secure name server 14." (*Johnson* 6:50-59.) In light of *Johnson*'s stated intention of limiting access for security purposes, it makes little sense for the servers of *Johnson* to register domain names in the public DNS to expand access. Because the proposed combination of *Johnson* with RFC 1034 would undermine *Johnson*'s intended purpose, the rejection should be withdrawn. *See* M.P.E.P. § 2143.01.

In view of the above, *Johnson* does not disclose or suggest "a first device associated with a secure name and an unsecured name," either alone or in combination with RFC 2131, RFC 1034, and RFC 2401. Thus, the rejection of claim 1 should be withdrawn.

B. Independent Claim 2

Independent claim 2 recites, among other things, "a second device having a secure name" and "from [a] first device, sending a message to a secure name service." For at least the reasons in Patent Owner's previous Response, (Response at 71), and those discussed above with regard to claim 1, *Johnson*, alone or in combination with RFC 2131, RFC 1034, and RFC 2401, does not disclose a "secure name" or a "secure name service." Thus, *Johnson* in view of RFC 2131, RFC 1034, and RFC 2401 does not render obvious claim 2.

C. Dependent Claims 3-16 and 18-23

Claims 3-16 and 18-23 depend directly or indirectly from claim 2 and are patentable for at least the reasons discussed above with respect to claim 2 and in Patent Owner's previous Response. (*Id.* at 68-71, 71-73.) In addition, the rejections of claims 3, 9-11, 13-16, and 21 should be withdrawn for the reasons set forth below.

D. Dependent Claim 3

Claim 3 recites, among other things, that "the secure name of the second device is a secure domain name." Both Requester and the Office contend that one of ordinary skill in the art would have been motivated to modify the secure name server of *Johnson* to register with a public DNS, "making it possible to locate the *secure name server 14* by name, for example, through the public resources of the Internet," as purportedly taught by RFC 1034. (Comments at 40, emphasis added; Second OA at 100-02.) By this reasoning, registering the secure name server 14 with a public DNS would convert what Requester and the Office claim is an "unsecured name" associated with the server to a "secure domain name." Even if one were to incorrectly assume that the secure name service and secure mail service are located on the same machine in the manner Requester and Office claim, (Req. at 277; First OA at 12, incorporating by reference the Request at 270-318), registering the purported "*unsecured* name" of the secure name server 14 with a public DNS does not somehow produce a "*secure* domain name" (emphases added). In other words, the purported "secure name" of the secure mail server 16 would not become a "secure domain name" by making it easier to locate the secure name server 14 publicly. Furthermore, as discussed above with respect to claim 2, *Johnson* does not disclose or suggest the claimed "secure name," and one of ordinary skill would not have been motivated to combine *Johnson* with RFC 1034 at least because the proposed combination would undermine *Johnson*'s intended purpose. For at least these reasons, *Johnson* in view of RFC 2131, RFC 1034, and RFC 2401 does not render obvious claim 3.

E. Dependent Claims 9-11 and 13-16

Requester and Office allege that claims 9-11 and 13-16 are rendered obvious by *Johnson* in view of RFC 2401. (Comments 41; Second OA at 103-04.) But, as discussed in Patent Owner's previous Response, one of ordinary skill in the art would not have combined the two references at least because combining the two would change the principle of operation in the *Johnson* system and render *Johnson* unsatisfactory for its intended purpose. (Response at 72-73.) Requester and the Office respond that the security mechanisms of *Johnson* would simply be modified to include the additional security mechanisms of RFC 2401. (Comments at 41; Second OA at 103-04.) Yet this would fundamentally change the principle of operation in *Johnson*. According to *Johnson*, the prior art "suffer[s] from the drawbacks of using known communication pathways, having known addresses, and some systems even transfer secure key information over the communication lines." (*Johnson* 4:55-59.) *Johnson* therefore advocates a method in which key information is not transmitted over the communication line. (*Id.* at 4:60-63, stating that "there is a need for an improved communication method which allows for encrypted information transfer to dynamic locations without transmitting the keys over the communication line.") The system taught in RFC 2401, however, involves sending security and key management traffic (i.e., ISAKMP) between the hosts and across the communication lines. (RFC 2401 17, stating that "[t]he SPD is used to control the flow of ALL traffic through an IPsec system, including security and key management traffic (e.g., ISAKMP) from/to entities behind a security gateway," 25, stating "a requirement for a security gateway to be configurable to pass IPsec traffic (including ISAKMP traffic) for hosts behind it.") Modifying *Johnson* with RFC 2401 would vitiate the very improvement *Johnson* advocates. As a result, the proposed combination of *Johnson* with RFC 2401 would change the principle of operation in *Johnson*, and the rejections are accordingly incorrect. *See* M.P.E.P. § 2143.01.

F. Dependent Claim 21

Claim 21 recites, among other things, an "unsecured name." In light of the Office's new arguments regarding the "unsecured name" discussed above with respect to claim 1, the rejection of claim 21 should be withdrawn.

G. Independent Claims 24, 26, 28, and 29

Although of different scope, independent claims 24, 26, 28, and 29 recite features similar to those discussed above in connection with claims 1 and 2, as discussed in Patent Owner's previous Response. (Response at 73-75.) Thus, for reasons similar to those discussed above with respect to claims 1 and 2, and for the reasons set forth in the previous Response, *Johnson*, alone or in combination with RFC 2131, RFC 1034, and RFC 2401, does not render obvious claims 24, 26, 28, and 29. (*Id.* at 68-70, 73-75.) The Office's new arguments regarding the "unsecured name," recited in claim 26, discussed above with respect to claim 1, are also incorrect for the reasons stated above.

H. Dependent Claims 25 and 27

Claims 25 and 27 depend from claims 24 and 26, respectively, and are patentable for at least the reasons discussed above with respect to claims 24 and 26, and for the reasons set forth in Patent Owner's previous Response. (*Id.* at 73-75.) The Office's new arguments regarding the "unsecured name," recited in claim 27, discussed above with respect to claim 1, are also incorrect for the reasons stated above.

X. Secondary Considerations Weigh Against Obviousness

As VirnetX noted in the Response, even if the Office had established a prima facie case of obviousness regarding any of the claims of the '181 patent (which it has not), there is substantial evidence to rebut any finding of obviousness. (*Id.* at 75-77.) Specifically, VirnetX presented evidence showing that the claimed inventions addressed a long-felt need, succeeded where others have failed, have been commercially successful, were contrary to accepted wisdom at the time of the invention, were met with skepticism by those skilled in the art, and received praise from others in the field. (*Id.*)

The Office did not weigh any of the objective evidence of nonobviousness against the facts on which the Office based its obviousness determinations—it simply concluded that the objective evidence does not "preclude[]" any of the rejections. (Second OA at 108, "[t]he Examiner has considered these 'secondary considerations' but doesn't see any evidence that precludes use of any of the above maintained prior art rejections.") This is not the correct standard. The Office erred with its conclusory analysis because "each piece of rebuttal evidence should not be evaluated for its ability to knockdown the *prima facie* case[; but rather all] of the competent rebuttal evidence taken as a whole should be weighed against the evidence supporting the *prima facie* case." M.P.E.P. § 716.01(d) (further explaining that "[f]acts established by rebuttal evidence must be evaluated along with the facts on which the conclusion of a *prima facie* case was reached, not against the conclusion itself."). The Office failed to weigh Patent Owner's substantial objective evidence against the Office's evidence of obviousness, and it further failed to "identify the reason(s) . . . [why the] evidence of commercial success [was] not convincing." *Id.* Accordingly, Patent Owner's objective evidence was incorrectly disregarded. Because the objective evidence detailed at length in Patent Owner's previous Response outweighs the Office's insubstantial and often conclusory grounds for its obviousness determinations, the rejections under 35 U.S.C. § 103 should be withdrawn. (Response at 75-77.)

The obviousness rejections are particularly deficient in light of the continued commercial success of the claimed inventions since VirnetX filed its last Response. As explained in the Response, Microsoft, Aastra, Mitel, and NEC have all entered into patent licensing agreements with VirnetX that include the '181 patent. (*Id.* at 77.) SafeNet, a leading provider of Internet security technology that is the de facto standard in the VPN industry, similarly entered into a portfolio license with the original owner of the '181 patent. (*Id.*) Microsoft was also found to willfully infringe two of the Munger family patents, leading to a damages award of over $100 million. (*Id.*) And recently, on November 6, 2012, the Eastern District of Texas found claims in four of the Munger family patents valid and infringed by Apple, with the jury's damages award exceeding $368 million. (*See* Ex. A-10 at 1; Ex. A-30 at 1-2.)

Simply put, VirnetX's evidence of commercial success, in addition to its other objective evidence set forth in its prior Response, rebuts any finding that the claimed inventions would have been obvious. (Response at 75-77.)

XI. Conclusion

For at least these reasons, VirnetX requests reconsideration and withdrawal of the rejections in the Second Office Action and confirmation of the patentability of all of the claims of the '181 patent.

VirnetX notes that the Second Office Action contains a number of assertions and allegations, including those concerning the disclosure, claims, and cited art. VirnetX does not subscribe to any assertion or allegation in the Second Office Action regardless of whether it is addressed specifically herein.

Please grant any extension of time and charge any required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 18, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

APPENDIX - LIST OF EXHIBITS

EXHIBIT	DESCRIPTION
A-10	Verdict Form from *VirnetX, Inc. v. Apple Inc.,* No. 6:10-CV-417 (E.D. Tex. November 6, 2012).
A-28	Response to Office Action in U.S. Application No. 11/679,416 dated October 8, 2012.
A-30	Final Judgment Pursuant to Fed. R. Civ. P. 54(b) from *VirnetX, Inc. v. Apple Inc.* No. 6:10-CV-417 (E.D. Tex. February 28, 2013).

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
	Control No.: 95/001,949
Victor Larson et al.	
	Group Art Unit: 3992
U.S. Patent No. 8,051,181	
	Examiner: Dennis G. Bonshock
Issued: November 1, 2011	
	Confirmation No.: 4522
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Supplemental Declaration of Angelos D. Keromytis, Ph.D.

I, ANGELOS D. KEROMYTIS, declare as follows:

1. I have been retained by VirnetX Inc. ("VirnetX") for the above-referenced reexamination proceeding. I understand that this reexamination involves U.S. Patent No. 8,051,181 ("the '181 patent"). I further understand that the '181 patent is assigned to VirnetX and that it is part of a family of patents ("Munger patent family") that stems from U.S. provisional application nos. 60/106,261 ("the '261 application"), filed on October 30, 1998, and 60/137,704 ("the '704 application"), filed on June 7, 1999. I understand that the '181 patent is a continuation of U.S. application no. 10/702,486 (now U.S. Patent 7,188,180), which is a divisional of U.S. application no. 09/558,209 filed April 26, 2000 (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent 6,502,135, "the '135 patent"). The '135 patent is a continuation-in-part of U.S. application no. 09/429,643 (now U.S. Patent 7,010,604), which claims priority to the '261 and '704 applications.

2. I have reviewed the '181 patent, including claims 1-29. I have also reviewed a Request for *Inter Partes* Reexamination of the '181 patent filed by Apple Inc. ("Requester" or "Apple") with the U.S. Patent and Trademark Office ("The Office") on March 28, 2012 ("Request" or "Req.") as well as the exhibits accompanying the Request. Additionally, I have reviewed an Order Granting Request for *Inter Partes* Reexamination of the '181 patent ("the Order") mailed on June 4,

2012 and an Office Action ("First Office Action") mailed on June 4, 2012.[1] In addition, I have reviewed VirnetX's response filed on September 4, 2012, and Comments by Apple, filed on October 22, 2012. I have also reviewed an additional Office Action mailed on January 16, 2013 ("Second Office Action" or "Second OA").

3. I have been asked to supplement my previous declaration to discuss certain issues raised in the Comments and the Second Office Action. My findings are set forth below. As in my September 2012 Declaration, my opinions are from the perspective of one of ordinary skill in the art as of the effective filing date of the '181 patent.

I. QUALIFICATIONS

4. My professional background and qualifications are stated in the September 2012 Declaration and are reflected in my curriculum vitae, appended to that declaration. Although I am being compensated at my standard rate of $500/hour for my work on this declaration, the compensation in no way affects the statements in my declaration.

II. STATUS OF THE '181 PATENT CLAIMS

5. I understand that the Office has maintained the rejections identified in Issues 1, 3-11, and 13 based on *Beser*, *Mattaway*, *Lendenmann*, *Provino*, *H.323*, and *Johnson*, either alone or in combination with additional references. I have been asked to consider and supplement my previous findings as to how one of one of ordinary skill in the art would have understood the '181 patent and the asserted references at the time of the priority date of the '181 patent as it relates to the maintained rejections.

1. *Beser*

6. I understand that the Office and Requester argue that the "first device" recited in claim 1 can be interpreted to be both first network device 14 and end-point device 24 in *Beser*. (Second OA at 18, quoting Comments at 5.) I also understand that claim 1 requires that particular actions be performed by "the first device" and "the second device." *Beser*'s first network device 14, however, is clearly a different device than end-point device 24. (*See Beser* Fig. 1.) Moreover, incorporating first network device 14 and end-point device 24 into a single device would render *Beser*'s tunneling scheme ineffective, because the *Beser* system aims to hide the IP address of end-

[1] The First Office Action incorporates nearly all of the Request by reference. For that reason, when I sometimes refer to "the Request" or "the Requester" I am also referring to the First Office Action or the Office.

point device 24, and it would not be able to do so if the end-point device 24 was a part of the same device as first network device 14.

7. I also understand that the Office contends that *Beser* teaches using encryption in combination with tunneling. (Second OA at 20.) I disagree. *Beser*'s "Background of the Invention" section includes three separate paragraphs discussing three different prior art communication methods, each of which uses encryption. (*Beser* 1:54-2:35.) *Beser* ends each of these paragraphs explaining how the use of encryption in these systems is undesirable because of an increased computational burden. (*See, e.g., id.* at 1:58-67, 2:12-17, 2:33-35.) Then, after consistently associating encryption in these prior art systems with an increased computational burden, *Beser* states in the subsequent "Summary of the Invention" section that "[t]he method and system described herein may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication *without an increased computational burden*," i.e., without encryption. (*Beser* 3:4-9, emphasis added.) *Beser* also discloses that the addresses of the ends of the tunneling association are "hidden" not using encryption, but instead using the "negotiation" process of step 118 that ensures that the addresses of the ends of the VoIP association are not included in the data packet address fields. (*See, e.g., id.* at 11:59-12:16.) In my opinion, a person of ordinary skill at the time of the priority date of the '181 patent would not looked to combine encryption with the tunneling described in *Beser*.

8. I also understand that the Office asserts that *Beser*'s tunneling associations use encryption. (Second OA at 23, citing *Beser* 11:22-25). I disagree. *Beser* discloses that "IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." (*Beser* 11:22-25.) But these "IP 58 packets" being described in this portion of *Beser* are not a part of what the Office points to as corresponding to the alleged secure communication link. Rather, the "IP 58 packets" described in *Beser* are sent as part of step 114, which is a communication between first network device 14 and trusted-third-party network device 30. (*Id.* at 11:9-25.) Thus, this communication is not sent between the alleged first device and the alleged second device.

2. *Mattaway*

9. I understand that the Office and Requester point to two different messages in *Mattaway*, the <CONNECT REQ> message and the <CALL> message, as disclosing a "message . . . of the desire[] to securely communicate," as recited in claim 1. In my opinion, neither message in *Mattaway* can be the recited message because neither is a message "of the desire[] to securely

communicate." For example, tables 6 and 8 of *Mattaway* explain that a <CONNECT REQ> message includes the following data entries, along with a brief explanation of what is included in each data entry:

Data Entry	**Comment**
WPP_CONNECTREQ	WPP message identifier
sid	Session ID
version	Version of the webphone
callType	Call type 0:EMAIL/1:IPCALL
partyEmailAddr	E-mail address of person to call
email Addr	E-mail address of caller
IPAddr	IP Address
connectState/connectStatus	0: No Webphone; 1: Online; 2: Offline; 3: Reconnect; 4: Perm_Reconnect

(*Mattaway* 36:45-65, 39:1-35, showing Tables 6 and 8.) None of the data entries included in the <CONNECT REQ> mention anything about security and, thus, the <CONNECT REQ> message cannot be a message "of the desire[] to securely communicate." Likewise, the <CALL> message is also not a message "of the desire[] to securely communicate." Tables 6 and 8 of *Mattaway* also explain that a <CALL> message includes the following data entries:

Data Entry	**Comment**
WPP_CALL	WPP message identifier
Sid	Session ID
Version	Version of the webphone
email Addr	E-mail address of caller
IPAddr	IP Address
userinfo	FirstName, LastName, alias, emailAddr, street, apt., city, state, country, postalCode, phone, fax, company

Just like those included in the <CONNECT REQ> message, the data entries in the <CALL> message also indicate nothing about security. Thus, the <CALL> also cannot be the recited message "of the desire[] to securely communicate."

10. I also understand that the Office maintains that *Mattaway* discloses a "secure name," as recited in claim 1. (Second OA at 31-33.) I disagree. A person of ordinary skill in the art at the time of the invention would have understood that "secure names" are those names used to communicate securely that are resolved by a secure name service (i.e., a service that both resolves a name into a network address and further supports establishing a secure communication link). The connection server 26 in *Mattaway,* by contrast, is a conventional name server of the type distinguished by the '181 patent specification and does not qualify as a "secure name service" that can resolve "secure names." Instead, when provided with an e-mail address of a callee's device, connection server 26 merely returns an IP address, if one is associated with the e-mail address. (*Mattaway* 18:30-19:9, Fig. 16A.) *Mattaway* does not disclose that the connection server 26 provides any further support for establishing a secure communication link. Accordingly, its operation is conventional, it is not a "secure name service" in the context of the '181 patent, and the e-mail addresses disclosed in *Mattaway* are not "secure names."

11. Moreover, *Mattaway* does not disclose that the alleged secure name—the encrypted e-mail address "eemailAddr" entry of Table 9—is associated with what the Office relies upon as the first device. Rather, the "eemailAddr" entry is sent from the global server to webphone 1536 (the alleged first device) as a part of the <USER INFO REQ> message. (*Mattaway* 22:65-23:5, 40:27.) *Mattaway* does not disclose that this "eemailAddr" entry is the e-mail address of the alleged first device or is at all associated with the alleged first device. By comparing the comments for the "eemailAddr" entry of Table 9, which read simply "encrypted email address," with the comments for the "emailAddr" entry of Table 8, which explain that it is the "email address of [the] caller" (i.e., the alleged first device), it is clear that the "eemailAddr" entry is different from the "emailAddr" entry included in the other messages, which is the e-mail address that corresponds to the caller.

3. *Lendenmann*

12. I understand that the Office now relies in part on the CDS-specific section of *Lendenmann* as disclosing the claim 2 features of "sending a message to a secure name service" and "receiving a message containing the network address." (Second OA at 62-63.) This section of *Lendenmann* does not relate to the RPC feature otherwise relied upon by the Office.

13. *Lendenmann* expressly differentiates between various types of communications in DCE. *Lendenmann* explains that its "OSF DCE components use three distributed computing models:" (1) the client/server model, (2) the remote procedure call model, and (3) the data sharing model. (*Lendenmann* at 8-9.) *Lendenmann* illustrates the client/server model as a request/response system of communication:

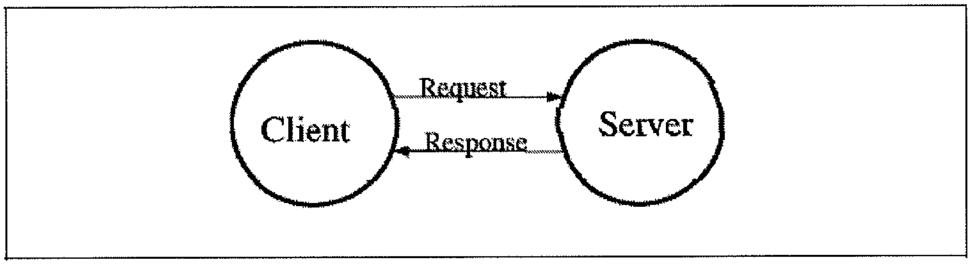


Figure 4. Client/Server Model

(*Id.* at 8.) The CDS-specific section of *Lendenmann* explains that the CDS "follows the client/server model." (*Id.* at 29.) It specifies that the CDS clerk "receives a request from [a] DCE application." (*Id.*) The CDS clerk then searches for the requested information. (*Id.* at 29-30.) Finally, the clerk "passes the requested data to the client application." (*Id.* at 30.) All of this language is consistent with the client/server model discussed in Figure 4, reproduced above. (*Id.* at 8.) *Lendenmann* does not refer to this simple lookup procedure referred to as an RPC or "data sharing" model communication.

14. This procedure in the CDS-specific section of *Lendenmann* stands in sharp contrast to the binding process required for initiating RPCs. As I explained in my previous declaration, the binding process involving the CDS during RPC setup identifies servers to the client based on functional criteria other than server names, whereas a CDS in the client/server model returns a network address "when given a name." (C*ompare id.* at 172-85 *with id.* at 21.) A person of ordinary skill in the art would have understood that these two embodiments—the client/server model and the RPC model—are incompatible because they use fundamentally different methods of resolving network addresses for use in DCE communications.

4. *H.323*

15. I understand that the Office asserts that an endpoint having a token-protected alias address corresponds to the "first device associated with a secure name" of claim 1, and that these token embodiments allegedly disclose "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." (Second OA at 80-81; Req. at 213.) I disagree, because in the

token embodiments, the alleged "second device" does not perform any functions that correspond to the features assigned to it in the claim.

16. For example, in the security token embodiment of *H.235*, Endpoint A (the alleged second device) initially sends a regular ARQ message to its gatekeeper to resolve the address of the gateway. (*H.235* at 28.) In the ACF message, the gatekeeper then returns the gateway's address and the security token containing the E.164 phone number of POTS-B (the alleged first device). (*Id.*) Next, Endpoint A sends a SETUP message to the gateway with the security token, and the gateway sends the security token back to the gatekeeper for deciphering. (*Id.* at 28-29.) This ends *H.235*'s disclosure. (*Id.*) None of these messages are sent from the alleged second device (Endpoint A) and received at a network address corresponding to the secure name associated with the alleged first device (POTS-B).

17. I also understand that the Office argues that a "request to communicate" sent by a calling endpoint (i.e., the alleged second device) in these embodiments corresponds to a "message . . . of the desired to securely communicate," as recited in claim 1. (Second OA at 81.) But in the token embodiments, the calling endpoint never sends a request to communicate desiring the use of a protective token to a called endpoint. Rather, the tokens are wielded by the called endpoint (i.e., the alleged first device) and used in combination with a gatekeeper so that a calling endpoint cannot obtain the called endpoint's transport address and communicate directly with the called endpoint. Indeed, *H.323* describes its tokens as "provid[ing] privacy by shielding an endpoint's Transport Address and Alias address information *from a calling party*." (*H.323* at 38; *see also H.235* at 28, "Assume that EPA [Endpoint A] is trying to call POTS-B, and POTS-B does not want to expose its E.164 phone number to EPA.") Called endpoints simply register their tokens with their gatekeepers and use the gatekeepers to shield them from calling endpoints. (*H.235* at 28-29; *H.323* at 38.)

18. I further understand that the Office and Requester additionally rely on "negotiations" in an *H.235* IPSEC embodiment involving an endpoint and a gatekeeper as disclosing the claim feature of "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." (Second OA at 82-83; Req. at 215-16, quoting *H.235* at 30-31.) I disagree.

19. The Office and Requester argue that in this IPSEC feature, "the endpoints can negotiate the use of IPSEC for the H.245 channel" during the SETUP and CONNECT exchange in establishing an *H.245* control channel, as shown in Figure 23 of *H.323*, reproduced below. (Second OA at 82.)

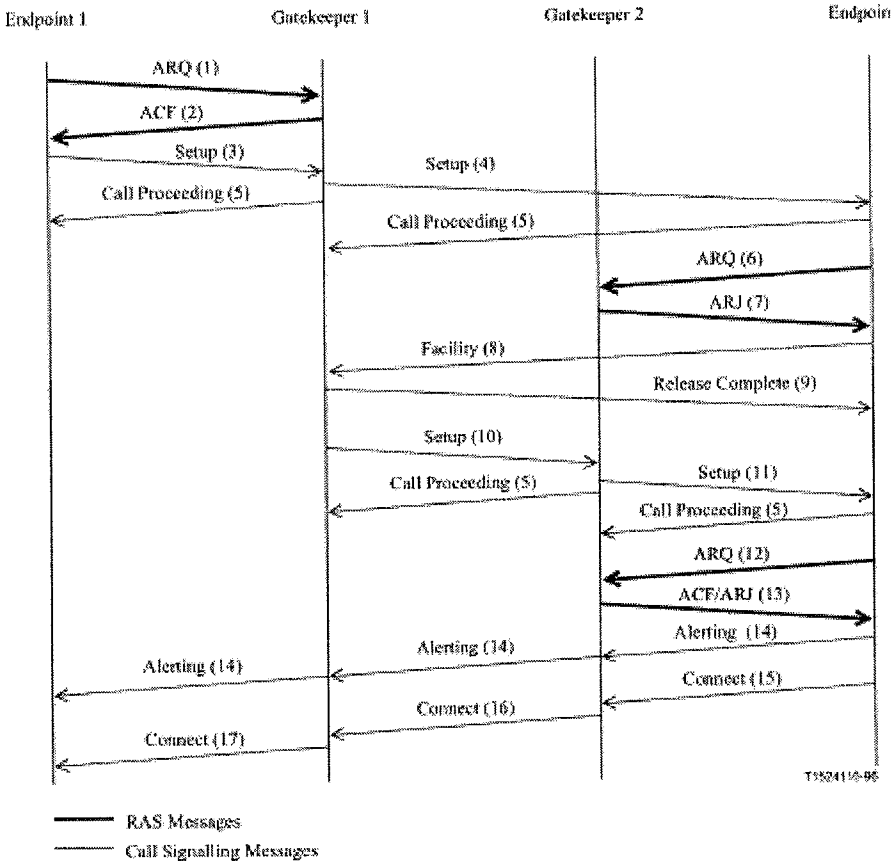


Figure 23/H.323 – Both endpoints registered – Both Gatekeepers routing call signalling

(*H.323* at 51, Fig. 23, showing setup and connection of an *H.245* control channel.) A person of ordinary skill in the art, however, would have understood that the "negotiations" relied upon by the Office and Requester do not correspond to "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device."

20. At least sixteen of the seventeen different messages shown and described in Figure 23 are either sent from an endpoint to a gatekeeper, or from a gatekeeper to an endpoint—not from the second device to the first device, as required by the claim. (*Id.* at Fig. 23; *cf.* "Alerting (14).") For example, *H.323* specifies that for Requester's alleged SETUP exchange, "Gatekeeper 1 shall return a Call Signalling Channel Transport Address of itself in the ACF (2) [to Endpoint 1]. Endpoint 1 then sends the Setup (3) message using that Transport Address." (*Id.* at 50.) As a result, a person of ordinary skill in the art would have understood that the Setup (3) message is sent from Endpoint 1 to Gatekeeper 1, and therefore does not correspond to the claim 1 feature of a message from a second

device that is received at a network address corresponding to the secure name associated with the first device.

21. A person of ordinary skill in the art would also have understood that the Setup (4) message does not correspond to "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device." (*See id.* at 51, Fig. 23.) With respect to Figure 23, *H.323* specifies that "Gatekeeper 1 then sends the Setup (4) message to the well-known Call Signalling Channel Transport Address of Endpoint 2." Thus, the Setup (4) message is sent from Gatekeeper 1 to Endpoint 2, and also cannot correspond to the claim 1 feature of a message from a second device that is received at a network address corresponding to the secure name associated with the first device. The other messages cited by Requester, such as the ARQ(6) and ACF(7) messages, are also only sent between an endpoint and a gatekeeper. (*See id.* at 51, Fig. 23.)

22. I also understand that the Office further contends that a "request for the session initiation . . . followed then either by an accepted or rejected decision by the other network end" corresponds to "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device," as recited in claim 1. (Second OA at 83.) I disagree. As shown in Figure 23 and described in the accompanying text, the Endpoint 1 initiates a session by interacting exclusively with Gatekeeper 1 during the "ARQ (1)/ACF (2) exchange." (*H.323* 50-51.) Then, for the accept/reject decision, "[i]f Endpoint 2 wishes to accept the call, it initiates the ARQ(6)/ACF(7) exchange with Gatekeeper 2," illustrating that this process is nothing more than an exchange of messages between Endpoint 2 and Gatekeeper 2.

23. In its rejection of claim 2, I understand that the Office relies on the IPSEC feature of *H.235* to show "a network address associated with the secure name of the second device." (Second OA at 84-85.) I disagree.

24. The only address relied upon in the quoted passage of *H.323* is a "well-known" transport address relating to a call signalling channel of Endpoint 2. (*H.323* at 50, "well-known Call Signalling Channel Transport Address.") A "transport address" is simply a basic network address with a TSAP identifier. (*Id.* at 8, defining "transport address.") *H.323* does not associate the well-known call signalling channel transport address with any name of an endpoint at all, much less a "secure name." (*Id.* at 50.) Rather, a person of ordinary skill the art would have understood that it is not associated with any particular "secure name," given that *H.323* describes it as "well-known." (*Id.*)

25. I understand that the Office also relies on the security token embodiment of *H.235* as disclosing "from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device," as recited in claim 2. I disagree. In this embodiment, Endpoint A does not send any "message requesting a network address *associated with the secure name* of the second device" because POTS-B has shielded its E.164 phone number (the alleged "secure name") from Endpoint A with the security token. (*Id.*) *H.323* explains that security tokens act to "obscure or hide destination addressing information." (*Id.*) The POTS-B device wields a security token because "POTS-B does not want to expose its E.164 phone number to [calling Endpoint A]." (*Id.*) As a result, rather than requesting a name associated with POTS-B's E.164 phone number, Endpoint A instead sends an ARQ to the gatekeeper to resolve the address of the Gateway between POTS-B and Endpoint A. (*H.235* at 28, the address "*as represented by its alias/GW*," emphasis added.)

26. I understand that claim 9 recites "automatically initiating the secure communication link after it is enabled." I also understand that the Office and Requester argue that the feature of "dynamically" updating an endpoint's security policy within the IPSEC embodiment corresponds to these claim features. (Second OA at 89.) I disagree. At that point in the IPSEC embodiment, no secure communication link is being initiated, let alone already been "enabled," as recited within the claim. Rather, *H.235* explains that the endpoints continue to have significant non-automatic authentication hurdles before any IPSEC-protected communications are enabled or subsequently initiated. (*H.235* at 30.) For example, *H.235* specifies that "person-to-person Q&A" and "user-to-user authentication" are involved in negotiating the characteristics of the channel "before any H.245 packets are transmitted." (*Id.*) Thus, a person of ordinary skill in the art would not have understood this embodiment to correspond to "automatically initiating the secure communication link after it is enabled," as recited in the claim.

III. CONCLUSION

27. I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 or Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the '181 patent.

28. Executed this 15th day of March 2013 in New York, New York.

Dated: March 15, 2013

/Angelos D. Keromytis/
Angelos D. Keromytis

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U. S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No. 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PETITION SEEKING WAIVER OF 37 C.F.R. § 1.943 FOR PATENT OWNER'S RESPONSE TO OFFICE ACTION OF JANUARY 16, 2013

Pursuant to 37 C.F.R. § 1.183, Patent Owner VirnetX Inc. ("VirnetX") requests that the Director waive the requirement of 37 C.F.R. § 1.943(b) limiting Patent Owner's responses to 50 pages in length. Specifically, VirnetX requests that the Office accept its 56-page response to the January 16, 2013, Office Action ("Office Action" or "OA").[1] VirnetX is submitting this petition concurrently with its response.

Rule 1.943(b) states that "[r]esponses by the patent owner and written comments by the third party requester [cannot] exceed 50 pages in length, excluding . . . reference materials." 37 C.F.R. § 1.943(b). VirnetX requests that the Director waive the page limit requirements of § 1.943(b) and permit VirnetX to submit an Office Action response containing 56 pages so that it can comprehensively address all the issues raised by the Examiner in the Office Action. Specifically, the Office Action adopted 11 grounds of rejection based on 11 different combinations of references proposed by third-party requester Apple Inc. ("Apple") in its request for reexamination. In doing so, the Office Action, itself 110 pages in length, relied on and incorporated by reference 293 pages of Apple's request and 48 pages of accompanying claim charts. (*See* OA at 5-12.) The 110-page Office

[1] The listed page and word count excludes the pages and words that constitute the "amendments, appendices of claims, and reference materials" as the Office has interpreted that language of 37 C.F.R. § 1.943(b).

Action also contains additional positions and arguments further to those presented in the request and accompanying claim charts. (*See* OA at 13-110.)

VirnetX's response seeks to comprehensively address all of the issues raised in the Office Action. Because of the numerous issues raised in the 110-page Office Action and the incorporation by reference 293 pages of Apple's request and 48 pages of accompanying claim charts, VirnetX requests that the Office accept its response that has 56 pages. VirnetX has made every effort to pare down its response, but submits that limiting its response to 50 pages would severely compromise its ability to fully address the issues raised in the Office Action.

With its response, VirnetX is also submitting a declaration by Dr. Keromytis, an expert. The declaration discusses how one of ordinary skill in the art would have understood the references cited in the Office Action. Given its content, VirnetX does not believe that the declaration counts towards the page limit. Nevertheless, should the Office decide to include portions of the declaration in the page count for the response, VirnetX requests that the Office waive the requirements of Rule 1.943(b) and permit it to submit this declaration with its response. Indeed, even if the Office were to count the declaration towards the page limit, the total number of pages representing the response and the declaration would still be substantially less than corresponding portions of the 293 single-spaced pages of Apple's request and 48 pages of accompanying claim charts relied upon and incorporated by reference in the 110-page Office Action.

For the foregoing reasons, VirnetX requests that the Office grant this petition and accept its Office Action response, which contains 56 pages and exceeds the page count limitations imposed by 37 C.F.R. § 1.943(b).

To the extent that entry and consideration of this petition requires suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. In addition, a petition fee of $1,930 is being submitted with this petition. If there is any other fee due in connection with the filing of this petition, please charge the fee to Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 18, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Joseph Edwin Palys./Connie Sisk
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION IN REEXAM PROCEEDING	1824	1	1930	1930
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
	Total in USD ($)			**1930**

Electronic Acknowledgement Receipt

EFS ID:	15282499
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Connie Sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	18-MAR-2013
Filing Date:	28-MAR-2012
Time Stamp:	14:47:27
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1930
RAM confirmation Number	1536
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		TransmittalCoS.pdf	468493 f00aa965db014a5a4b4fb81cb2539e1b143380b7	yes	3
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Reexam Miscellaneous Incoming Letter		1	1	
	Reexam Certificate of Service		2	3	
Warnings:					
Information:					
2	Response after non-final action-owner timely	Response.pdf	844519 8fe85e84282d3fdc3a019f76e906640a86cc1a5c	no	56
Warnings:					
Information:					
3	Reexam Miscellaneous Incoming Letter	AppendixExhibits.pdf	16069 0a9965b2015a67515a248ae463976fcfa6464c30	no	1
Warnings:					
Information:					
4	Reexam Miscellaneous Incoming Letter	ExA10.pdf	64057 db9edcf12bdd38ebb4400eb5505cec3c4019058b	no	3
Warnings:					
Information:					
5	Reexam Miscellaneous Incoming Letter	ExA28.pdf	492528 2a74c111b94b18b660c1a56e333e5ee8324f65fd	no	13
Warnings:					
Information:					
6	Reexam Miscellaneous Incoming Letter	ExA30.pdf	75150 9482ff2565aa492d00d6efcc493b467069d9b6f8	no	3
Warnings:					
Information:					
7	Reexam Miscellaneous Incoming Letter	Keromytis.pdf	589300 571f908fa2804ba326e3f6cd12b3f867fff4a377	no	11
Warnings:					
Information:					
8	Reexam Miscellaneous Incoming Letter	PetitionExtraPage.pdf	101889 ebfd8cce7d7aee6b4ea20f29dbb1cdfaab8eef63	no	2

Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	30354 4a1f53271075dd9d2e64de84f7cc0bb44cdd0247	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2682359		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of	Control No.: 95/001,949
Patent No. 8,051,181	Examiner: Dennis G. Bonshock
Inventors: Larson et al.	Group Art Unit: 3992
For: METHOF FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	Confirmation No.: 4522

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

THIRD PARTY REQUESTOR'S PETITION IN OPPOSITION TO PATENT OWNER'S PETITION TO REOPEN PROSECUTION

Third Party Requestor Apple Inc. ("Petitioner") presents views in opposition to the petition served by the Patent Owner on March 18, 2012 (March 18 Petition).

I. Relevant Background

On June 12, 2012, the Office commenced *Inter Partes* Reexamination Control No. 95/001,949 (the '949 proceeding) concerning U.S. Patent No. 7,051,181 (the '181 patent) on the basis of a request filed by Apple as a Third Party Requestor.

On June 4, 2012, the Office issued an Order ("Order") and Office Action ("First Office Action") imposing rejections on claims 1-29 of the '181 patent.

On September 4, 2012, Patent Owner responded to the Office Action and petitioned the Office to waive the 50-page limit for a Patent Owner response. The response filed by Patent Owner was approximately 115 pages in length.

On October 22, 2012, Petitioner timely filed written comments on Patent Owner's response to the Office Action. Petitioner's written comments complied with the 50-page limit specified in 37 CFR 1.943(b).

On December 5, 2013, Third Party Requestor filed a petition to align the schedules of several related proceedings, including Reexamination Control Nos. 95/001,788 and 95/001,189.

On January 16, 2013, the Office issued an Action Closing Prosecution ("ACP") maintaining the rejections previously imposed on all 29 claims of the '181 patent. Each rejection of each claim in the ACP was on the same statutory basis, and relied upon the same prior art, as the corresponding rejection of that claim in the First Office Action.

On January 22, 2013, Patent Owner petitioned the Office for a 1-month extension of the time period for its response, which was granted by the Office on January 25, 2013.

II. Requested Action

Petitioner requests the Director to dismiss Patent Owner's March 18 petition in its entirety, as each of the rejections imposed in the ACP rests on the same statutory basis, and relies on the same prior art, as the corresponding rejection in the Office Action.

III. Argument

Patent Owner's current petition represents yet another attempt to indirectly challenge the merits of the rejections imposed by the Office, and to simply delay conclusion of this reexamination proceeding. The Office should reject this transparent attempt to delay conclusion of these reexamination proceedings.

In its Petition, Patent Owner asserts the ACP was premature because certain "issues have not been fully developed" and because it believes the Office "introduces several new bases for its rejections." March 18 Petition at 2. Patent Owner contends that as a result, it has not received "sufficient opportunity to respond to these newly adopted positions" and that "prosecution should therefore be reopened." *Id.*

Patent Owner's assertions are remarkable in light of the record in this proceeding. Inspection of that record demonstrates that Patent Owner has been provided an exhaustive opportunity to present its views in opposition to the rejections of the claims of the '181 patent. For example, the Office allowed Patent Owner to file a response to the Office Action that was <u>more than twice</u> the length authorized by the rules. The Office also has twice granted extensions of time requested by the Patent Owner, giving Patent Owner in the aggregate <u>more than five months</u> to formulate and present its views to the Office. By contrast, Petitioner, within the 30 day period provided in the statute, provided its written comments on Patent Owner's response, and did so within the 50 page limit specified in the Rules. The Office, thus, has afforded Patent Owner opportunities far beyond those ordinarily permitted by the Rules for responding to the rejections of the claims of the '181 patent, and it is disingenuous for Patent Owner to assert it has not been provided an adequate opportunity to respond to the rejections.

The standards that govern imposition of an ACP compel the conclusion that the ACP was proper. The Manual of Patent Examining Procedure (MPEP), at § 2671.02, specifies that:

> [I]t is intended that the second Office action in the reexamination proceeding will ordinarily be an ACP. The criteria for issuing an ACP is analogous to that set forth in MPEP § 706.07(a) for making a rejection final in an application.

MPEP § 706.07(a), in turn, specifies:

> [A] second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims, nor based on information submitted in an information disclosure statement filed.

MPEP § 1207.03 similarly explains "what may constitute a new ground of rejection," explaining that a rejection is not a new ground of rejection if:

> [T]he basic thrust of the rejection remains the same such that an appellant has been given a fair opportunity to react to the rejection . . . . Where the statutory basis for the rejection remains the same, and the evidence relied upon in support of the rejection remains the same, a change in the discussion of, or rationale in support of, the rejection does not necessarily constitute a new ground of rejection. (emphasis added)

Thus, where a rejection rests on the same statutory grounds, relies on the same prior art and the same evidence, it generally will not constitute a new grounds of rejection. Moreover, a different expression of the grounds of the rejection, particularly in response to contentions made by a patent owner in its response to a first Office Action is also not a "new grounds" of rejection.

Under these standards, the ACP in this proceeding was clearly proper. Each rejection maintained in the ACP rests on the same statutory basis and the same prior art relative to the corresponding rejection imposed in the first Office Action. Moreover, no new evidence was introduced or relied upon by the Office in the ACP to support any of the rejections – the rejections are each supported by the same evidence relied upon in the first Office Action.

Patent Owner implicitly recognizes this in its March 18 petition. Nowhere does Patent Owner suggest that any of the statutory basis or prior art used in any of the rejections in the First Office Action are different than the rejections imposed in the ACP. A simple review of the ACP shows that the Office has properly maintained the rejections it previously imposed in the First Office Action based on its conclusion that Patent Owner's response to those rejections was unpersuasive. On this basis alone, the Office must dismiss the present petition.

Patent Owner's criticisms of the ACP are simply another attempt to circumvent the rules and procedures that govern *inter partes* reexamination proceedings. In this petition, Patent Owner again presents a series of criticisms of the basis of the rejections, but again casts these criticisms as formal deficiencies associated with imposition of the ACP. The Office should disregard these criticisms, as they are baseless.

First, Patent Owner contends that the Office changed its position on the *Mattaway* reference. Specifically, Patent Owner asserts that in the Office Action, the Office cited the <CONNECT REQ> message in *Mattaway* as disclosing the "receiving, at a network address corresponding to the secure name associated with the first device, *a message from a second device of the desire[] to securely communicate with the first device.*" March 18 Petition at 2 (emphasis in original). Patent Owner contends that the Office has changed its position in explaining that the desire to securely communicate is received at the first device in the form of the <CALL> message.

Patent Owner is incorrect. The explanation provided in the ACP by the Office was plainly in response to Patent Owner's disingenuous criticism of what *Mattaway* teaches. For example, Patent Owner argued that in *Mattaway* there was no disclosure that the desire to securely communicate represented by the <CONNECT REQ> message was ever "received at a network address corresponding to the secure name associated with the alleged first device." Response at 21. In response, the Comments of Third-Party Requestor, as well as the ACP, point out that the <CONNECT REQ> message, i.e., the "desire[] to securely communicate," is received at the first device in the form of the <CALL> message. This is confirmed by Figure 17A (which Patent Owner wrongly states stands for the opposite proposition), as <CALL> is shown as the step (Step 8) following the <CONNECT REQ> and <CONNECT ACK> (Steps 6 and 7A) messages identified in the Request. This is also confirmed by the *Mattaway* specification. See, e.g., *Mattaway* at 23:42-24:42. Thus, the ACP was simply responding to Patent Owner's baseless and inaccurate criticism of the Office Action.

Second, Patent Owner contends that the Office has "adopted a new basis" in identifying the "secure name" disclosed in *Provino*. Patent Owner's assertion is again incorrect. Here, Patent Owner simply cherry-picks an out-of-context statement from the ACP to support its contention that the Office has "drastically changed its rejection." March 18 Petition at 4-5. The manner in which the Request, the First Office Action and the ACP refer to the showing of a "secure name" in *Provino* has remained entirely consistent throughout this reexamination. This is exemplified by the explanation in the Request, which was incorporated by the Office into both the First Office Action and the ACP:

> Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." *See* Provino at 8:67-9:5.

Request at 170. The above-quoted language in the Request, which was incorporated into the Office Action and confirmed by the ACP, has consistently identified the Domain Name in the Nameserver 32 (which is resolvable into an IP address, i.e., an "integer Internet address") as acting on a "secure name" as specified in the '181 patent claims. Thus, the Office has not elaborated its position at all, but simply maintained the basis of the rejection that had been previously imposed. See, e.g., Request at 168-171; ACP at 71-73.

Third, Patent Owner incorrectly claims that the Office has adopted "a new rejection" based on *Lendenmann* for "sending a message . . . requesting a network address associated with the secure name of the second device" element of claim 2. On this point, Patent Owner first incorrectly contends that *Lendenmann* shows that the components of its system use three different models of distributed computer: client server model, the remote procedure call ("RPC") model, and the data-sharing model. *Lendenmann* at 8-9. In reality, the *Lendenman* system does not show three distinct modes of operation, but blends elements of the three models to create the features of its system. For example, as consistently explained in the Request, First Office Action, Comments, and ACP, an application client making an RPC call in the *Lendenmann* system locates an application server to handle the call, not by iteratively searching through servers, but by requesting an address for a server from a CDS. Request at 112-14; First Action at 12; ACP at 60-61. For this element, *Lendenmann* thus blends the RPC and client server models.

Relying on this incorrect portrayal of what *Lendenmann* actually teaches, Patent Owner then contends that the Office has "changed course" in the ACP by relying on the showing in *Lendenmann* of use of a Cell Directory Server ("CDS") to return a network address, contending that the CDS is based on a client server model, while the rejection imposed in the First Office Action was based on part of *Lendenmann* showing use of an RPC model.

Patent Owner is again incorrect. The Office clearly relied on the CDS showing in *Lendenmann* in the First Action when imposing the rejections of the claims. For example, in the First Action, the Office stated, "Lendenmann teaches a [CDS] that stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource (see page 21)." First Action at 12. Only by ignoring the Office's clear reliance on the CDS embodiment of *Lendenmenn* in the First Action can Patent Owner assert that the ACP imposes a new rejection. Patent Owner's arguments are simply nonsensical. The Office has not imposed a new rejection; Patent Owner merely mischaracterizes the rejections the Office actually made.

<u>Fourth</u>, Patent Owner asserts that the Office, through its rejection based on *Johnson,* has adopted "a new rejection that is at odds with the Office's previous statements." March 18 petition at 6-7. In particular, Patent Owner contends that the Office's reliance on the "dynamic address of the secure mail server 16" as disclosing the "unsecured name" of the claims of the '181 patent is "an entirely different element than was relied upon in the First Action. This is incorrect.

In the Request, the Petitioner demonstrated that *Johnson* describes <u>two</u> alternatives in which an unsecured name is disclosed, including one in which "the secure name server may be accessed or selected according to the secure server's <u>name</u>." Request at 273-74 (emphasis added). The Request further explained that in this embodiment, it would be known to use a domain name registered in the public DNS system. Request at 274. The Examiner agreed that this disclosure in *Johnson* satisfies the "unsecure name" requirement of the relevant claims of the '181 patent as it found that the publicly registered domain name (the public "address") was an unsecure name. First Action at 20 (citing *Johnson* at 11:21-37); ACP at 98 (citing *Johnson* at 11:21-37). Thus, Patent Owner's claim that the

Examiner adopted a new rejection by identifying the dynamic address—rather than the registered public domain address—as the "unsecure name" of the relevant claims of the '181 patent is simply false. Patent Owner's inability to understand the actual basis for the Examiner's rejections does not mean that the basis of those rejections has changed.

Thus, Patent Owner's assertions are baseless. The Office did not change the basis of rejection of any of the claims between the First Office Action and the ACP. Instead, the record demonstrates unequivocally that it has maintained the same rejection of the same claims on the same statutory grounds over these references as was imposed in the First Office Action. The Office also did not change what it had found each of *Mattaway*, *Provino*, *Lendenmann*, and *Johnson* to teach. Instead, it simply pointed out, in response to Patent Owner's incorrect assertions, why those references actually taught what the Office and Requestor said it did. Patent Owner does not contend in its Petition that the Office has relied on any "new evidence" or changed the statutory basis of the rejections of any of the claims relative to how those rejections were set forth in the Office Action. Consequently, the Office's findings are presumptively not a new ground of rejection within the meaning of MPEP § 1207.03. Indeed, as the MPEP expressly provides, "a change in the discussion of, or rationale in support of, the rejection does not necessarily constitute a new ground of rejection." MPEP § 1207.03 Accordingly, the Director should dismiss the Patent Owner's March 18 Petition to Reopen the Prosecution.

The Director is authorized to charge the fee specified in 37 CFR § 1.17(f) to Deposit Account No. 18-1260. In addition, the Director is authorized to charge any other fee he deems necessary to Deposit Account No. 18-1260.

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requestor

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile

March 27, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of	)	Control No.: 95/001,949
	)	
Patent No. 8,051,181	)	Examiner: Dennis Bonshock
	)	
Inventors: Larson et al.	)	Group Art Unit: 3992
	)	
For: METHOD FOR ESTABLISHING	)	Confirmation No. 4522
SECURE COMMUNICATION LINK	)	
BETWEEN COMPUTERS OF	)	
VIRTUAL PRIVATE NETWORK	)	

Mail Stop *Inter Partes* Reexam
ATTN: Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF SERVICE

I hereby certify that a copy of the Third Party Requestor's Petition in Opposition to Patent Owner's Petition to Reopen Prosecution has been served in its entirety by First Class Mail on the following:

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
901 New York Avenue, NW
Washington, DC 20001-4413

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requestor

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile
March 27, 2013

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Karen L. Knezek.
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION IN REEXAM PROCEEDING	1824	1	1940	1940
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**1940**

Electronic Acknowledgement Receipt

EFS ID:	15369383
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Karen L. Knezek.
Filer Authorized By:	
Attorney Docket Number:	41484-80200
Receipt Date:	27-MAR-2013
Filing Date:	28-MAR-2012
Time Stamp:	16:20:52
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1940
RAM confirmation Number	3338
Deposit Account	181260
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Receipt of Petition in a Reexam	Petition_response.pdf	124274 b6ad0a7bbb18efaf87b7a8624a0083badf6b2a75	no	7
Warnings:					
Information:					
2	Reexam Certificate of Service	Certificate_of_service.pdf	97595 b2a1d073ccdeb586dfe9989e7c76e7ea2c87829e	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	29861 e85e4960568f0f3dff8a90052dcc6646c1ed7b8a	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	251730	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of	)	
U.S. Patent No. 8,051,181	)	Control No.: 95/001,949
Larson et al.	)	Group Art Unit: 3992
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. § 1.947

Mail Stop **Inter Partes Reexam**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On September 4, 2012, Patent Owner filed an overlength response ("First Response") to the June 4, 2012 Office action ("First Action"). On October 22, 2012, Requester filed a 45-page response with comments ("Comments") on Patent Owner's response. On January 16, 2013, the Office issued an Action Closing Prosecution ("ACP") that found claims 1-29 of U.S. Patent No. 8,051,181 ("the '181 patent") unpatentable. On March 18, 2013, the Patent Owner filed a second overlength response ("Second Response") and a petition under 37 C.F.R. § 1.183 seeking to waive the page limit rule for that response. Although the Office has not acted on the page-limit waiver as of the date of this submission, Requester provides these comments now to expedite conclusion of this proceeding. Requester believes no fee is due for this response, but authorizes the Director to debit any fee determined to be necessary from Deposit Account No. 18-1260.

I. General Comments on Errors that Pervade Patent Owner's Second Response

Throughout its Second Response, Patent Owner repeatedly makes several errors that should be given no weight in this proceeding.

First, Patent Owner asserts that several of the Office's positions in the ACP are new and require reopening of prosecution. This claim is baseless. As the Requester demonstrated in its March 27, 2013 Opposition to Patent Owner's Petition to Reopen Prosecution, each of the supposedly "new bases for [] rejections" issued by the Office are not new at all, but rather are identical to positions previously taken by the Office in its First Action or responses to unpersuasive criticisms by the Patent Owner. Indeed, the Second Response simply rehashes arguments Patent Owner and its expert presented earlier, advances unsupportable *legal* theories about the claims, or attempts, for the first time, to address issues that were ripe for response after the First Action. The Examiner should simply ignore these incorrect contentions. In this regard, Requester notes that Patent Owner submitted a Supplemental Declaration of Angelos D. Keromytis, Ph.D with its Second Response, but did not establish good and sufficient reasons why this affidavit is necessary or could not have been presented earlier. Under 37 CFR § 1.116(e), this affidavit should be barred. Indeed, the only basis Patent Owner presents for admitting this affidavit is that the Office has adopted new rejections, which, as explained herein and in Requester's March 27, 2013 Opposition, is demonstrably false.

It is the Requester's understanding that the Office will consider a petition to strike or exclude a Supplemental Declaration under 37 CFR § 1.116(e) to be premature if the Examiner has not yet issued an action determining whether to enter the declaration.[1] Rather than burdening the Office with such a petition now, Requester notes that Patent Owner has not shown good cause for submitting the declaration and that the Examiner should not admit or consider the new evidence or arguments presented in the Supplemental Declaration.

Second, as in its First Response, many of Patent Owner's arguments are premised upon alternative constructions of the claim elements, not adopted by the Office, that read limitations from the '181 specification into the claims. In particular, Patent Owner repeatedly argues that the Office should ignore Patent Owner's representations made during the prosecution of the '181 patent and during a reexamination of the '180 patent concerning the terms "secure name" and "unsecured name," and should instead construe those terms to include unclaimed limitations based on embodiments discussed in the specification. Not only did Patent Owner belatedly raise these claim construction arguments for the first time in the Second Response, Patent Owner's criticisms show that it fundamentally misunderstands the Office's policy of giving the claims their broadest reasonable construction. In proceedings before the Office, a patent owner must amend the claims to effectively exclude subject matter actually encompassed by the claim language. *See* MPEP § 2111 (explaining that under the broadest reasonable construction practice used in PTO proceedings, ". . . applicant has the opportunity to amend the claims during

[1] *See* Decision on Petitions in 95/001,788 at 8 (Mar. 26, 2013).

prosecution, [and that] giving a claim its broadest reasonable interpretation will reduce the possibility that the claim, once issued, will be interpreted more broadly than is justified.") (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984).

Patent Owner's arguments in this case vividly demonstrate why this rule is followed – all of Patent Owner's arguments before the Office seek to impermissibly import unclaimed limitations, requirements, meanings, disparagements or disclaimers into the claims in order to narrow their scope and avoid the prior art, now that the claims have been found – based on their actual language – to encompass what is disclosed in or rendered obvious from the prior art. *See* M.P.E.P. § 2111.01(II); *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969). If Patent Owner is unsatisfied with the meaning of the claims as they are written, Patent Owner should seek to amend the claims to correspond to the meaning(s) Patent Owner desires them now to have instead of asking the Office to simply ignore its well-established practices in construing a claim's scope. Allowing the Patent Owner to recast its claims without actually amending them would violate the Office's well-established practice of requiring a patentee to expressly incorporate limitations in the claim language to effectively limit their scope in these proceedings, and would prevent the Office and Requester from evaluating the newly claimed subject matter for compliance with 35 U.S.C. § 112. Consequently, Patent Owner's requests that the Office depart from its well-established practices must be uniformly rejected.

II. The Rejections of the Claims Were Proper

A. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-12, 14, 15, and 17-29 Based on *Beser* (Issue 1).

1. Independent Claim 1

In the ACP, the Office correctly maintained its determination that *Beser* anticipates claim 1. In response, Patent Owner asserts *Beser* does not teach a system that discloses (1) "a first device," "a second device," "a message from [the] second device of the desire[] to securely communicate with the first device" or "sending a message over a secure communication link from the first device to the second device." Second Response at 2-6. Each of these assertions is incorrect.

a. *Beser* Discloses "a First Device," "a Second Device," and "a Message from [the] Second Device of the Desire[] to Securely Communicate With the First Device"

The Office correctly found that *Beser* discloses both "a first device" and "a second device." ACP at 17-19. For example, *Beser* illustrates its system in Figure 1, which shows two edge routers (14 and 16), each linked to a different communication device (24 and 26, respectively). These devices are used to communicate with each other over a secure network established, *inter alia*, using the trusted third party networking device (30). *Beser* at Fig. 1. Either the communication devices (items 24 and 26) or the edge routers (items 14 and 16) can qualify as a "first" and "second" devices, respectively, under the plain meaning of the claims, which impose <u>no restrictions</u> on the properties or capabilities of the "first" or "second" devices.

The Office also correctly found that *Beser* shows a method where a "message from a second device of *the desire* to securely communicate with the first device" is "received, at a network address corresponding to the secure name associated with the first device." ACP at 18. For example, the Office correctly found that *Beser* shows an originating device (items 24 or 14) (a "second device") that sends a message requesting a connection with a destination device (items 16 or 26) (a "first device") to a trusted third network device. *Beser* at 11:25-32. The trusted third party network device routes the request to the destination edge router (16) associated with the destination communication device (26) (a "network address corresponding to the secure name associated with the first device"). *Id.* If the connection is authorized, the trusted third party network device facilitates establishment of a secure communication link between the originating and destination communication devices. *Id.* Finally, the Office correctly found that *Beser* discloses that, after the secure link is established, *a different message* (*e.g.*, packets containing data representing a VOIP communication) is sent from the originating device to the destination device using the secure communication link ("sending a message over a secure communication link from the first device to the second device").

Patent Owner has not disputed any of these findings. Instead, Patent Owner asserts the Office and the Requester have improperly read the claim language, mischaracterized its arguments or misapplied the law of anticipation. These assertions are spurious.

First, Patent Owner italicizes several passages in claim 1 (*e.g.*, a "first device," the "desire to securely communicate" "from the second device") and asserts these are not shown in *Beser*. Second Response at 2. These contentions border on the incomprehensible. For example, Patent Owner may be contending that because *Beser* does not label its originating device as a "second" device or does not label its destination device as a "first device," *Beser* cannot anticipate the claims. This semantic distinction is meaningless, and must be rejected. Under the plain meaning of claim 1, the originating device shown in *Beser* (the device that sends the message) qualifies as a "second" device within the meaning of the claims because it sends a message requesting a connection to a destination device, which qualifies as a "first device" within the meaning of the claims.

Next, Patent Owner contends the Office erred by finding that the claims merely require a message to be sent between the two devices. Here, Patent Owner mischaracterizes the Office's findings and ignores what is actually shown in *Beser*. Specifically, *Beser* shows a first message containing a request to communicate with a destination device is sent by the originating device. *Beser* at Fig. 6. This meets the claim requirement of a "message of the desire to securely communicate" with the destination device. Then, *Beser* shows that a different message is sent from the trusted third party device to the edge router providing access to the destination communication device which starts the process of negotiation of the secure connection. *Id.* *Beser* also shows a different message (*e.g.*, the data representing the content of the VOIP communication) is sent by the originating device to the destination device *after* the secure connection is established. *Id.*; *id.* at 4:44-54. Thus, even under Patent Owner's reading of the claims, *Beser* plainly anticipates this feature of claim 1. Of course, there is nothing in claim 1 that excludes the messages being sent in the *Beser* systems. Moreover, based on the claim language, the first message may have the same content as a subsequent message.

Patent Owner also contends the Request and the Office improperly conclude that multiple devices may qualify as "first" or "second" devices. This again is a spurious complaint. Nothing in the claims precludes a "device" from being an edge router, a communication device or both working in conjunction. In fact, the '181 patent itself illustrates the claimed systems by showing devices on a local network communicating with remote destination using edge routers – precisely what is shown in *Beser*. Compare *Beser* at Fig. 1 to '181 Patent at 51:15-29 and Fig. 28. Patent Owner also disputes the Office's conclusion that the various devices shown in *Beser* may "at any particular point" qualify as a first or second device. In reality, there is nothing in the claims that precludes reading the claims as encompassing these various embodiments described in *Beser*. For example, nothing in the claim precludes intermediary devices on a network path from being a first or second "device." And Patent Owner's complaint that the Office and the Request "never identified the alleged first device and the alleged second device in *Beecher*" is simply false. Second Response at 3. All of these documents point out precisely how features of the *Beser* precisely match the requirements of the claims. For example, as explained in the Request, First Action, and ACP, *Beser* discloses both a "first device" and a "second device" that meet the limitations of the claims. Request at 27-29; First OA at 6-7, ACP at 18-19 (citing *Beser* at 11:26-12:19). In the *Beser* systems, when an "originating telephony device" makes a request to securely communicate with a "terminating telephony device," the request is brokered by intermediary devices, including a "first network device," a "second network device," and a "trusted-third-party device." *Beser* at Fig. 6. The request is a message containing the "unique identifier" for the "terminating telephony device." *Beser* at 11:25-32. When the "trusted-third-party device" receives the message, it uses the "unique identifier" to look up a public IP address for a "second network device" that is associated with the "terminating telephony device," and then it sends the message requesting a secure connection to the "second network device." *Beser* at 11:26-32 ("A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at step 116. The second network device 16 is associated with the terminating telephony device 26."). The "second network device" receives the message requesting a secure connection and then negotiates the tunneling association for the "terminating telephony device." *Beser* at Fig. 6; 11:59-62. The result of the creation of the tunneling associating is that the "terminating telephony device" and the "originating telephony device" (the "first" and "second" devices) can send and receive messages over the secure connection. Thus, contrary to Patent Owner's assertions, the Office and Requester have not been "picking and choosing among different devices in *Beser*." Instead, they have been comparing <u>what is actually claimed</u> to <u>what is actually disclosed</u> in *Beser*.

Patent Owner's next contention is similarly flawed. Specifically, Patent Owner disputes the observation made in the Request and by the Office that there is no restriction in the claims precluding either the edge router or the communication device, or both working together, from being a first or a second device within the meaning of the claims. Second Response at 4. Patent Owner misunderstands this point, reading it as suggesting that a single device in the *Beser* system (*e.g.*, one edge router or one communication device) can be both a first and second device. The point made by the Office (and Request) is that either the communication device or the edge router or both working together can be <u>one device</u> within the meaning of the claims. That one device then will communicate securely with a <u>different</u> edge router/communication device/combination (the "second" device). Patent Owner's criticisms here can be disregarded.

Much of Patent Owner's argument rests on its belief that it is appropriate for the Office to read unclaimed limitations into the claims to distinguish them from the prior art. The Office has correctly rejected this theory. If Patent Owner wishes to exclude the subject matter described in *Beser* from the scope of its claims, it must amend those claims to contain language that expressly does so. As the claims presently read, they do not, and the rejections for anticipation by *Beser* are thus proper and should be maintained. Consequently, the Office correctly found that *Beser* discloses "a message from [an originating telephony device] of the desire to securely communicate" is received "at [the] network address corresponding to the [unique identifier] associated with [the terminating telephony device]." Similarly, the Office correctly found that *Beser* shows "sending a message over a secure communications link from the [terminating telephony device] to the [originating telephony device]." Accordingly, *Beser* describes a system that provides "a first device," "a second device," and "a message" as required by the claims.

b. *Beser* Discloses "Sending a Message Over a Secure Communication Link from the First Device to the Second Device."

The Office correctly maintained its determination that *Beser* discloses "sending a message over a secure communication link." In response, Patent Owner presents the same arguments it presented in response to the First Action; namely, that *Beser* does not describe a "secure communication link" because (1) "the broadest reasonable interpretation of secure communication link requires encryption, and *Beser's* tunneling association is not encrypted" and (2) "even if the Office maintains that a secure communication link does not require encryption, *Beser*'s tunneling association still is not a secure communication link." Second Response at 5. For reasons the Office has already conveyed, both of these contentions are incorrect.

Patent Owner first repeats its flawed reading of *Beser*; namely, that it "teaches away from using encryption in its tunneling system." *Id.* As the Office correctly determined, the passages cited by Patent Owner do not "teach away" from the use of encryption in IP tunneling associations. Rather, what those passages explain is that only in <u>certain high data volume</u> situations can the use of encryption demand additional computational capacity to implement. As was explained in Requester's comments and the ACP, the claims are not limited to high data volume applications, but encompass communications of any magnitude. ACP at 20. The cautionary observations in *Beser* about <u>certain</u> types of data communication applications are thus irrelevant to what is <u>actually claimed</u>.

Moreover, Patent Owner again mischaracterizes the teachings in *Beser* about use of encryption in IP tunneling. As the Office explained, *Beser* consistently and repeatedly points out that use of legacy encryption techniques in IP tunneling schemes is conventional and ordinarily should be used. The Office found that *Beser* "specifically teaches utilization of encryption in combination with the tunneling, where this tunneling is being used as an additional means of making the channel for transmission secure . . . ." ACP at 20 (emphasis added). Although *Beser* does indicate that there may be practical challenges using encryption in some circumstances, this concern is not an express teaching to never use IPSec or other encryption-based IP tunneling models, or that the *Beser* techniques are only an alternative to using encryption—a conclusion with which the Patent Office has consistently agreed. ACP at 21; *see also* Action Closing Prosecution of 95/001,788 ("'788 ACP") at 32.[2] Instead, *Beser*'s tunneling scheme is to be "used in combination with legacy encryption to ensure data security." ACP at 20.

Patent Owner also contends that "even if a secure communication link [does] not require encryption" then "*Beser's* tunneling scheme still does not disclose a secure communication link." Second Response at 6. Yet, as explained in the Request, the inventive tunneling method shown in *Beser* "is designed to protect the integrity of the private IP address and ensure the anonymity of the terminating devices." Request at 26. Moreover, the Office correctly found that *Beser*'s systems "provide[] an additional layer of security by not only encrypting data but hiding the source and destination IP addresses." ACP at 21. Accordingly, *Beser* discloses "a secure communication link." Patent Owner offers no new arguments, but merely repeats the same baseless assertions it made in its First Response about *Beser* not providing secure communication links. Those assertions are not only refuted by the express teachings in *Beser*, they rest on unclaimed limitations and features of the claims. The Office properly rejected Patent Owner's assertions when they were made in the previous Patent Owner response, and should do so again. Thus, because the Office properly found that *Beser* discloses all the limitations of claim 1, its finding of anticipation of claim 1 was proper and should be maintained.

2. Independent Claim 2

The Office correctly found that *Beser* discloses every limitation of independent claim 2. Patent Owner does not present any new or distinct response to the rejection of claim 2, but

[2] U.S. Patent No. 7,418,504 to Larson, which is at issue in the '788 reexamination, is derived from the same applications as U.S. Patent No. 8,051,181 to Larson.

instead refers to its arguments regarding claim 1. Because claim 1 was properly rejected, the Office's finding of anticipation of claim 2 was proper and should be maintained.

3. Dependent Claim 4

The Office correctly found that *Beser* discloses every limitation of dependent claim 4. Patent Owner disagrees, arguing that *Beser*'s "unique identifier" does not "indicate anything about security." Second Response at 7. Patent Owner's argument is an immaterial variation of the argument it made in its First Response that *Beser* does not disclose a "secure name service" which the Office properly rejected. *See* First Response at 12-13; ACP at 21-22.

Patent Owner's assertions also are refuted by the teachings of *Beser*. As explained in the Request, the first network device and the trust-third-party device can recognize the "unique identifier" as being secure and can then implement protocols to obfuscate it from discovery by untrusted parties:

> "For each transfer of a packet from the first network device 14 to the trusted-third-party network device 30, the first network device 14 constructs and IP 58 packet. . . . <u>The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12</u>." Request at 36 (quoting *Beser* at 11:13-25).

Thus, because *Beser* recognize that security must be implemented for certain "unique identifiers," *Beser* discloses that "the secure name indicates security."

In addition, *Beser*'s "unique identifier" is clearly within the scope of Patent Owner's construction of the term "secure name." As the Office observed in the <u>First Action</u>, Patent Owner asserted during prosecution of the related '180 patent that the term "secure name" could be construed to include "*a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number*." First Action at 5. Requester has explained that *Beser*'s "unique identifier" could be a non-standard domain name such as a secure domain name or it could be an E.164 phone number, and the Office has adopted this conclusion. Order at 5-6; Request at 35-36. As described above, the *Beser* systems can recognize that security must be implemented for certain "unique identifiers"—which would include secure domain names or phone numbers. Thus, *Beser* discloses that "the secure name indicates security." Consequently, the Office's rejection of claim 4 as anticipated by *Beser* was proper and should be maintained.

4. Dependent Claim 5

The Office correctly found that *Beser* anticipates every limitation of dependent claim 5. In response, Patent Owner admits that *Beser* discloses encrypting messages sent to the trusted-third-party device, but argues that, for the "the message containing the network address associated with the secure name of the second device," *Beser* does not disclose "receiving the message in encrypted form." Second Response at 7-8. Patent Owner's argument is again an immaterial variation of its unpersuasive assertions on this point in its First Response, which the Office properly disregarded. Again, Patent Owner's argument is based on an incorrect reading of *Beser*. As the Office explained, *Beser* discloses encrypting "IP packets 58 [*sic*]," which would include any of the packets sent in establishing the secure communications link that contained the "unique identifier," "public IP 58 addresses," or "private IP 58 addresses." ACP at 23. In response to such a query, the third-party-trusted device would return a message containing the "public IP 58 address" associated with the "unique identifier" of the query. Thus, *Beser* discloses that the message received by the first network device can be encrypted. Accordingly, *Beser* discloses that "the message containing the network address associated with the secure name of the second device" is "receiv[ed] . . . in encrypted form." Consequently, the Office's rejection of this claim was proper and should be maintained.

5. Independent Claims 24, 26, and 29

In response to the rejection of claims 24, 26, and 29, Patent Owner presents no distinct responses from those offered in claim 1. Because the rejection of claim 1 was proper, the rejections of claims 24, 26, and 29 based on *Beser* also were proper and should be maintained.

6. Independent Claim 28

In response to the rejection of claim 28, Patent Owner presents no distinct response from those offered in claim 2. Because the rejection of claim 2 was proper, the rejection of claim 28 based on *Beser* was also proper and should also be maintained.

7. Dependent Claims 3, 6-12, 14-15, 17-23, 25 and 27

Patent Owner presents no distinct response to the rejection of claims 2-3, 8, 12, 14-15, 17 and 19-22 based on *Beser* relative to its response to the rejection of claim 2. Consequently, because the rejections of those claims were proper, the Office's rejections of claims 3-4, 8, 12, 14-15, 17 and 19-22 based on *Beser* were proper and should be maintained. Request at 35-45.

B. Response to Patent Owner's Arguments Regarding Rejection of Claims 1, 2, 6-9, 12-17, and 24-29 Based on *Mattaway* (Issue 3).

1. Independent Claim 1

Mattaway describes methods and systems for establishing a secure communication link between two devices across a public network such as the Internet. *See* Request at 68-72; ACP at 30-34. The Office correctly maintained its determination that *Mattaway* describes a system that anticipates claim 1. In its Second Response, Patent Owner asserts again that *Mattaway* does not teach a system that discloses (1) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, (2) "[a] first device associated with a secure name and an unsecured name" Second Response at 9-12. Both assertions are incorrect.

a. *Mattaway* Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"

Patent Owner's first response is that the Office has changed its position on what *Mattaway* teaches. Specifically, Patent Owner asserts that in the First Action, the Office cited the <CONNECT REQ> message in *Mattaway* as disclosing the "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." Second Response at 9. Patent Owner contends the Office has now taken a new position in explaining that the desire to securely communicate is received at the first device in the form of the <CALL> message. Patent Owner is wrong. The explanation provided by the Office in the ACP was plainly in response to Patent Owner's disingenuous criticism of what *Mattaway* teaches. For example, Patent Owner argued that in *Mattaway* there was no disclosure that the desire to securely communicate represented by the <CONNECT REQ> message was ever "received at a network address corresponding to the secure name associated with the alleged first device." Response at 21. In response, the Requester (and Office) pointed out that the <CONNECT REQ> message, *i.e.*, the "desire[] to securely communicate," is received at the first device in the form of the <CALL> message. This is confirmed by Figure 17A (which Patent Owner wrongly states stands for the opposite proposition), as <CALL> is shown as the step (Step 8) following the

<CONNECT REQ> and <CONNECT ACK> (Steps 6 and 7A) messages identified in the Request. This is also confirmed by the *Mattaway* specification. *Mattaway* at 23:42-24:42.

Moreover, the Request explained that after receiving the IP address of the first device, the second device may "directly establish the point-to-point Internet communications with the [first device] using the IP address of the [first device]." Request at 72; ACP at 33-34. *Mattaway* discloses these "point-to-point Internet communications" are accomplished by the second device "open[ing] up a socket" to the first device. *See Mattaway* at col.24, ll.15-30; ACP at 33-34. The second device transmits a "<CALL>" packet to the first device, to which the first device may, among other things, acknowledge or reject the call. *Mattaway* at col.24, l.11 – col.25, l.12; ACP at 33-34. Patent Owner simply ignores this observation in its response.

Patent Owner also asserts that neither the <CONNECT REQ> message nor the subsequent <CALL> message "include any information related to security." Second Response at 10; *see also id.* at 11. The Office properly rejected that theory because nothing in the claim language requires that the messages themselves have "information related to security." The process disclosed in *Mattaway* "enables the parties to converse in real-time, telephone quality, encrypted communication over the Internet and other TCP/IP based networks." *Mattaway* at col.25, ll.32-34; Request at 72; ACP at 34. Therefore, *Mattaway* discloses a message from the "second device" of the "desire to securely communicate" pursuant to claim 1. This reading of *Mattaway* is also consistent with Patent Owner's approach in concurrent litigation, where it has asserted that because Apple's "FaceTime calls are encrypted for secure communication . . . any request to make a FaceTime call is a request expressing the desire to securely communication using FaceTime." Exhibit A[3] at 2. Patent Owner cannot have it both ways, and its assertion that the message itself must "include . . . information related to security" must be given no weight in view of its contrary assertions on infringement against Requester.

b. *Mattaway* Discloses "A First Device Associated With A Secure Name and An Unsecured Name"

Patent Owner next asserts that *Mattaway* "does not disclose a secure name," because "those [are] names [that] are used to communicate securely that are resolved by a secure name

[3] Exhibit A constitutes Patent Owner's Evidence of Infringement against Requester filed with its Complaint in ITC investigation 337-TA-858, In re *Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing Same.*

service," and that "the connection server 26 of *Mattaway* . . . is a conventional server of the type distinguished by the '181 patent specification." Second Response at 11. These assertions can simply be ignored because they are predicated on Patent Owner's belief that the claims incorporate specific requirements regarding the claimed "secure name" which are not actually recited in the claims. As to the first point, the Office properly found that Patent Owner's representations regarding "secure name" here are inconsistent with those it made during prosecution when it told the Patent Office a "secure name" could be "as simple as a telephone number." ACP at 32. Patent Owner's contentions here also are entirely inconsistent with its assertions in concurrent litigation. Specifically, Requester asserted in an action it commenced in the ITC against Requester that:

> The secure name of the device is related to the caller's email address or, for Accused iPhones, the caller's telephone number. The Apple servers which facilitate the FaceTime function store a plurality of secure names and associated network addresses. A prospective caller's registration for FaceTime use using an email address or telephone number constitutes a request for registration of a secure name for the Accused Device used by the caller.

Exhibit A at 10 (emphasis added). As to the latter point—that *Mattaway's* servers are "conventional"—Patent Owner asks the Office to treat its "disclaimer" of conventional servers as an effective claim limitation that excludes subject matter which the language in the claims actually encompasses. *See* Second Response at 11-12. Because it has not proposed to amend its claims, these efforts to read limitations into them to exclude the embodiment of the "secure name" shown in *Mattaway* must be rejected.

Patent Owner also contends (again) that the secure name disclosed in *Mattaway* (an e-mail address) "is not associated with the first device." Second Response at 12. The Office correctly rejected this assertion in the ACP, explaining that "email addresses" are utilized in *Mattaway* to obtain IP addresses from the connection server, ACP at 31, and that a "user may use an alias to access the secured data under the firewall, where the secured data includes email addresses and IP addresse[s]." ACP at 32. The devices shown in *Mattaway* (webphones) are each required to register information as part of the <USER INFO REQ> message. *Mattaway* 22:65-23:5, 40:27. *Mattaway* thus discloses that information requested from the first device/Webphone client would include an encrypted email address. Accordingly, *Mattaway* discloses "a first device associated with a secure name and an unsecured name." The Office's rejection of claim 1 based on *Mattaway* thus, was proper and should be maintained.

2. Independent Claim 2

In the ACP, the Office correctly found that *Mattaway* discloses every limitation of dependent claim 2. In response, Patent Owner presents no distinct response to the rejection of claim 2 based on *Mattaway* relative to its response to the rejection of claim 1. Because the Office's rejection of claim 1 over *Mattaway* was proper, its rejection of claim 2 over *Mattaway* also should be maintained.

3. Independent Claims 24, 26, 28, and 29

In the ACP, the Office correctly found that *Mattaway* discloses every limitation of independent claims 24, 26, 28 and 29. In response, Patent Owner presents no distinct response relative to its response to the rejection of claim 1 over *Mattaway*. Because the rejection of claim 1 over *Mattaway* was proper, the Office's rejection of claims 24, 26, 28, and 29 over *Mattaway* also was proper and should be maintained.

4. Dependent Claims 7-9, 12-17, 25, and 27

In the ACP, the Office correctly found that *Mattaway* discloses every limitation of dependent claims 7-9, 12-17, 25, and 27. In response, Patent Owner presents no distinct response relative to its response to the rejection of claims 2, 24, and 26 over *Mattaway*. Because the Office's rejection of claims 2, 24, and 26 over *Mattaway* was proper, its rejection of claims 7-9, 12-17, 25, and 27 over *Mattaway* also was proper and should be maintained.

C. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3-4, 10-11, 18 and 23 Based on *Mattaway* in view of *Beser* (Issue 4).

1. Dependent Claim 4

In the First Office Action, the Office correctly found that *Mattaway* in view of *Beser* describes a system that would render claim 4 obvious to a person of ordinary skill in the art. In its First Response, Patent Owner asserted only that "*Beser* does not make up for the deficiencies noted above regarding *Mattaway's* disclosure." Response at 28-29. Understandably, the Office did not find this argument persuasive. Now, it its Second Response, Patent Owner contests <u>for the first time</u> the substantive findings set forth in the <u>First Action</u> regarding *Mattaway* in view of *Beser*, contrary to the requirements of 37 C.F.R. 1.951. *See* 37 C.F.R. 1.951 ("the patent owner may once file comments <u>limited to the issues raised in the Office action closing prosecution.</u>") Patent Owner's belated response should be disregarded.

Even if Patent Owner's belated response is considered, it should be rejected as unpersuasive. First, Patent Owner contends that *Beser* does not show that the unique identifier used in its schemes "indicates security." Second Response at 13. Yet, *Beser* plainly teaches that its scheme – in which the unique identifier plays a critical role – provides security, *inter alia*, through obsfucation of internal IP addresses of the originating and destination communication devices. *See* Request at 96. A person of ordinary skill in the art would have plainly recognized from that description that the unique identifier is associated with secure communications. Moreover, the Office did not rely on "conclusory" statements to support the rejection of claim 4. Second Response at 13. Instead, as explained in the Request, *Mattaway* recognizes the importance of using encrypted communications in its system to secure the data that is exchanged. Request at 96. *Beser* also recognized the importance of securing the data being transmitted in its system, and explained that a further measure of security could be achieved through obfuscation of the unique identifier, *i.e.*, the "secure name" of *Beser*. Request at 96. Thus, the Request explained in detail why a person of ordinary skill would have considered it obvious to use the obfuscation techniques described in *Beser* in which the unique identifier "indicates security" in the *Mattaway's* scheme, which, like *Beser*, emphasizes security. Thus, the Office's rejection of claim 4 was proper and should be maintained.

2. Dependent Claim 10

In the ACP, the Office correctly maintained its determination that *Mattaway* in view of *Beser* would have rendered claim 10 obvious to a person of ordinary skill in the art. Claim 10 recites "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." As explained in the Request, a person of ordinary skill in the art would have found motivation within *Mattaway* to modify the encrypted communications disclosed therein to incorporate additional mechanisms of protection in order to provide a more secure communication link. Request at 96-97; ACP at 51-53. That person would have found that *Beser* identified the same problem (improving security of network communications) and provided a solution to that problem; namely, to use a particular type of IP tunneling.

Again, rather than contesting any of these points in its First Response, Patent Owner now belatedly challenges these substantive findings that were set forth in the First Office Action. The Office should disregard these comments pursuant to Rule 951. Even if those comments are considered, they should be disregarded as being unpersuasive. Indeed, Patent Owner's only argument is premised on the assumption that the secure communication link disclosed in *Mattaway* could not include the communication link between the server that facilitates the secure communication link. Nothing in the description of *Mattaway* would preclude that embodiment. Accordingly, the Office's rejection of claim 10 was proper and should be maintained.

3. Dependent Claims 3, 11, 18, and 23

In the ACP, the Office correctly found that *Mattaway* in view of *Beser* discloses every limitation of dependent claims 3, 11, 18 and 23. In response, Patent Owner presents no distinct response relative to its response to the rejection of claim 2 over *Mattaway* in view of *Beser*. Accordingly, because the Office's rejection of claim 2 was proper, its rejection of claims 3, 11, 18 and 23 based on *Mattaway* in view of *Beser* also was proper and should be maintained.

D. Response to Patent Owner's Arguments Regarding Rejection of Claims 10 and 11 Based on *Mattaway* in View of RFC 2401 (Issue 5)

1. Dependent Claim 10

In the ACP, the Office correctly maintained its determination that *Mattaway* in view of RFC 2401 would have rendered claim 10 obvious to a person of ordinary skill in the art. Claim 10 recites "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." As explained in the Request, a person of ordinary skill in the art would have found motivation within *Mattaway* to modify the encrypted communications disclosed therein to incorporate additional mechanisms of protection in order to provide a more secure communication link. Request at 98-99; ACP at 54-55. That person also would have recognized that RFC 2401 addresses the same problem – improving security of networked communications – and provides a solution to that problem; namely, use of a particular type of tunneling.

Again, Patent Owner's belated comments should be disregarded as they were not presented in response to this ground of rejection when it was imposed in the First Office Action. They also should be rejected as being incorrect. Indeed, Patent Owner assertions are premised on the mistaken belief that the secure communication link disclosed in *Mattaway* could not include a communication link with the server that facilitates the secure communication link.

Nothing in the description of *Mattaway* precludes such a configuration. Accordingly, the Office's rejection of claim 10 was proper and should be maintained.

2. Dependent Claim 11

In the ACP, the Office correctly found that *Mattaway* in view of RFC 2401 discloses every limitation of dependent claim 11. In response, Patent Owner presents no distinct response relative to its response to the rejection of claim 2 based on *Mattaway* in view of RFC 2401. Accordingly, because its rejection of claim 2 was proper, the Office's rejection of claim 11 based on *Mattaway* in view of RFC 2401 also was proper and should be maintained.

E. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-9, 12-15, and 18-29 Based on *Lendenmann* (Issue 6).

1. Independent Claim 1

The Office correctly maintained its determination that *Lendenmann* describes a system that anticipates claim 1. In response, Patent Owner repeats and expands upon arguments it made in its First Response, namely that (1) *Lendenmann* does not teach a system that discloses "[a] first device associated with a secure name and an unsecured name" and (2) the Office has relied on "multiple unrelated features as corresponding to the 'first device' recited in claim 1." Second Response at 15-20. These arguments are not materially different from the arguments the Office previously found unpersuasive. They also rest on incorrect characterizations of *Lendenmann* and are inconsistent with Patent Owner's own representations before the Patent Office.

a. *Lendenmann* Discloses "A First Device Associated With A Secure Name and An Unsecured Name"

Patent Owner advances three different arguments as to why *Lendenmann* does not disclose a first device associated with a secure name and an unsecured name. Second Response at 16-18. Each argument should be disregarded.

First, Patent Owner contends the Office has misconstrued the terms a "secure name" and an "unsecured name. " The Office properly rejected this argument when Patent Owner made it in its First Response, and should do so again. Patent Owner's new theories about what its claims mean or do not mean, and how those claims relate to *Lendenmann* should be disregarded, not only because they are untimely pursuant to 37 C.F.R. 1.951, but because they ignore what the claims actually specify.

In its Second Response, Patent Owner strenuously disputes the Office's conclusions about the broadest reasonable construction of the terms "secure name" and "unnsecure name." The reason is simple – under the meanings employed by the Office, the claims encompass the systems described in *Lendenmann*, and are anticipated by this prior art.

For example, Patent Owner contends it was improper for the Office to use the Patent Owner's own representations about what the claim terms "secure name" and "nonsecure name" mean. Patent Owner is simply wrong – its own statements about these terms are highly probative evidence about what the terms do or do not reasonably encompass under their broadest reasonable construction.

As explained in the First Action and ACP, Patent Owner represented to the Office that a "secure name" may be any type of non-standard name. Under that interpretation, a "secure name" may be an X.500 name. ACP at 56; Request at 22; Order at 5 (Patent Owner asserted terms are not indefinite because a "secure name" could be "a secure non-standard domain name" or a "telephone number."). In response, Patent Owner asks the Office to disregard its previous representations that were made to secure allowance of these claims and analogous statements made during reexamination in the '180 patent, and instead import restrictions into the claims from particular examples in its specification. For example, Patent Owner contends that its prior statement that a "secure name" could be "a secure non-standard domain name" or a "telephone number" should be ignored because that statement "merely illustrate[s] exemplary differences between a 'secure name' and a 'secure domain name' in response to an indefiniteness rejection." Second Response at 16.

Patent Owner's statements were not limited as it contends. Rather, Patent Owner asserted that the term was not indefinite because one would recognize it could encompass "a secure non-standard domain name" or a "telephone number." The Office correctly found that because a X.500 name is a "non-standard domain name," it is a "secure name" within the meaning of the claims. Similarly, when Patent Owner's claims in a related patent (the '180 patent) were being rejected over the prior art, Patent Owner made unconditional statements about what the specification of the '180 patent (which is the same as the specification of the '181 patent) said a "secure" and "unsecure" name could be. As Patent Owner stated:

> The '180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a convention[al] domain name server using a secure domain name will result in a

> return message indicating that the URL is unknown ('180 patent at 51 :25-35) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name ('180 patent at 51:25-35).

Request at 22. These comments are probative here not only because Patent Owner advanced the same construction in the '180 reexamination proceeding that it advanced during prosecution of the '181 patent, but because these comments reflect Patent Owner's characterization of what the common specification of the '180 and '181 patents says these terms mean.

Patent Owner asks the Office to disregard those past statements, and instead read material limitations into the claims from specific examples shown in the specification. Patent Owner attempts to justify this request by asserting the construction used by the Office and Requester "removes all meaning of 'secure' and 'unsecure' from the claim terms." Second Response at 16. Patent Owner is incorrect. The meanings for these terms that Patent Owner advanced previously to the Office are not incompatible with the claim language. For example, claim 1 uses the term "secure name" to identify the destination of a message. *See* claim 1 ("receiving, at a network address corresponding to the secure name associated with a first device, a message from a second device"). Similarly, in claim 2, the term is used to identify a device. *See* claim 2 ("from the first device, sending a message to a secure name service, the message requesting a network address associated with a secure name of the second device…"). The use of "unsecure" or "secure" names to serve these identification functions is not incompatible with the claim language. In fact, Patent Owner actually uses the precise meaning it advanced during the prior proceedings in a dependent claim. Specifically, claim 23, which depends from claim 2, specifies that a "the secure name of the second device is a secure, non-standard domain name.") Thus, Patent Owner's assertions that the meanings used by the Office and in the Request for "unsecure" and "secure" names are somehow incompatible with its disclosure are simply false.

Patent Owner's examples of contradictions between its specification and the claim language can be easily rejected. For example, Patent Owner asserts that in one example shown in the '181 specification, a top-level domain name is replaced with a secure domain name in order to establish a secure communication link, and then after that communication link is terminated, the secure domain name is replaced with a non-secure domain name. Second Response at 16-17. This example has no relevance to what Patent Owner has actually claimed because there is no claim limited to this precise sequence of steps Patent Owner describes.

Patent Owner's arguments thus can be easily dismissed – they do not compare what is actually claimed to the prior art, but instead compare unclaimed features in the specification to the disclosure in *Lendenmann*. In fact, the example from the '181 specification cited by the Patent Owner here illustrates use of a non-standard domain name as a secure name to establish a secure connection. Moreover, under the broadest reasonable construction used by the Office, the claims do not necessarily exclude this "replacing" embodiment. *See* M.P.E.P. § 2111.01(II); *Superguide Corp. v. DirecTV Enterprises, Inc.*, 358 F.3d 870, 875, 69 USPQ2d 1865, 1868 (Fed. Cir. 2004) ("Though understanding the claim language may be aided by explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim. For example, a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment."). Nor is anything in Patent Owner's example inconsistent with the Office's determination that a "secure name" may be a non-standard domain name or a phone number. Simply put, if Patent Owner believes the claims as written are overly broad, it must amend those claims instead of attempting read unclaimed limitations from the specification into them.

Second, the Patent Owner argues *Lendenmann* does not disclose a device that has both a "secure name" and an "unsecure name." Specifically, while Patent Owner acknowledges that *Lendenmann* refers to both X.500 and DNS as naming schemes, it asserts there is no "nexus between X.500 names and secure communications" shown in *Lendenmann*. Second Response at 17. The Office has already rejected this argument, finding that "X.500 satisfies the requirement for a secure name, as the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address." ACP at 58. The Office also explained that the X.500 naming scheme of the DCE environment "is a secure, internal naming convention." ACP at 58 (citing Request at 105). For example, the Request explained that resolution of the X.500 names is controlled by the CDS, which is integrated into the security server of the X.500 system and will only complete an operation "if the user is authenticated and authorized." Request at 104. Thus, as explained in the ACP and the Request, DCE cells, as well as the objects within them, can have both an X.500 name (a "secure" name) and a DNS name (an "unsecure" name), and the Office correctly found that *Lendenmann* discloses "a first device associated with a secure name and an unsecured name."

Third, Patent Owner argues that *Lendenmman* does not disclose "secure" names because it does not "hid[e] Internet addresses" and does not disclose accessing Internet addresses outside of the DCE environment. Patent Owner's arguments can be dismissed based on the Office's construction of the term "secure name" and the actual teachings of *Lendenmann*.

A name may be found to be secure if it is stored in a secure location and whether it can be resolved by a conventional name server. X.500 names satisfy this definition. As *Lendenmann* explains, addresses in its system are hidden because queries to the CDS, which is integrated into the security server, are made within the confines of the DCE cell and can also be encrypted. ACP at 58-59. Further, whether the *Lendenmann* systems access Internet addresses outside of the DCE environment has no relevance to the question whether *Lendenmann* discloses a device having a "secure name" and an "unsecure name." *Lendenmann* presents the X.500 scheme, which is "a secure, internal naming convention," and the DNS scheme, which is a naming convention based on the public Internet DNS system is unsecure (*e.g.*, because conventional name servers are publicly accessible and resolve conventional domain names in a manner that provides no inherent security). Because Patent Owner's arguments are all based on improper claim constructions and a misunderstanding of the *Lendenmann* systems, the Office should disregard them and maintain the rejection of claim 1 as anticipated by *Lendenmann*.

b. *Lendenmann* Discloses "a First Device" as required by Claim 1

For the first time, Patent Owner asserts that *Lendenmann* does not disclose a "first device," contending that Office has improperly "mixed and matched" various elements of *Lendenmann* to find it discloses a "first device" specified in claim 1. Specifically, Patent Owner contends the Office and Requester have improperly combined features of the DCE cell, the CDS server, and the RPC server to meet the different limitations regarding the first device. Second Response at 18-19 (citing ACP at 56, 59 and Request at 106-08).

Patent Owner's arguments are based on its misunderstanding of the ACP and the Request. What the cited portions of the ACP and the Request explain is that either the DCE cell or the RPC server may be a "first device" due to the broad language used in claim 1. For example, *Lendenmann* shows that during the RPC binding process, an RPC client uses the name service interface (NSI) to make a request to the appropriate CDS server to get an address associated with a compatible RPC server, which can be identified by a DNS address or an X.500 address. Request at 106-07. The RPC client then sends a request to establish a communications channel to the RPC server in which it can request that security protocols be implemented.

Request at 107-08. Future communications between the RPC client and server are then secure. The first device thus can be either the RPC server or, if the client and server are in different DCE cells, the DCE cell to which the RPC server belongs. Because the RPC server is a part of that DCE cell, any communications sent to or from the RPC server will necessarily be sent to or from the DCE cell. Consequently, any "secure name" associated with the RPC server necessarily is also associated with the DCE cell, so the Office's rejection was proper and should be maintained.

2. Independent Claim 2

The Office correctly found that *Lendenmann* discloses every limitation of dependent claim 2, and thus anticipates this claim. Underpinning this determination was the observation that the systems described in *Lendenmann* can have a variety of configurations and capabilities. Indeed, Patent Owner admits this is the case. *See, e.g.*, First Response at 31-32 ("*Lendenmann*'s DC may include several different components, including security services, time services and directory services. [] It further discloses that a collection of machines, operating systems, and networks managed by a single set of DCE services constitutes a 'DCE cell.' At a minimum, a cell must contain a Security Server, a Cell Directory Server ('CDS'), and Distributed Time Servers. [] These separate components provide different services for establishing remote procedure calls (RPC's) between clients and servers."); *Id.* at 32 ("... *Lendenmann* describes three alternatives [for locating servers that provide services or applications over the DCE]: automatic, implicit or explicit binding. [] A client must then locate servers, for which *Lendenmann* also describes several alternatives: searching files, environment variables, or the CDS; or simply hard-coding a network address into an application.") Patent Owner thus admits that a person of ordinary skill reading *Lendenmann* would have recognized that it is describing not only a wide array of possible configurations of components, but that these different configurations also may exhibit a wide variety of functionalities.

Despite acknowledging the diverse and extensive teachings of *Lendenmann*, Patent Owner disputes that *Lendenmann* anticipates claim 2. Its challenges rest on a distorted reading of *Lendenmann* and an incorrect portrayal of what its claims encompass. Specifically, Patent Owner's arguments are premised on its belief that *Lendenmann* teaches three entirely unrelated models of distributed computing—the client server model, the remote procedure call ("RPC") model, and the data-sharing model—a view contradicted by Patent Owner's own characterizations of *Lendenmann* and by the explicit teachings in *Lendenmann*. Moreover, Patent Owner's assertions rest on a presumption that the claims are limited to specific examples described in the specification of the '181 patent. Patent Owner is incorrect on both points.

a. *Lendenmann* Discloses "Sending a Message to a Secure Name Service," "Receiving a Message Containing the Network Address," and "Sending a Message . . . Using a Secure Communications Link."

In the ACP, the Office correctly found that *Lendenmann* discloses the above-noted claim elements. In its First Response, Patent Owner argued that *Lendenmann* does not disclose "sending a message to a secure name service" and "receiving a message containing the network address." Now, in its Second Response, Patent Owner admits that these limitations are disclosed in *Lendenmann*, but argues that the Office has adopted a "revised argument" that improperly "mixes and matches" various features of *Lendenmann* to satisfy the limitations. *Id.* at 20.

The basis of the Office's rejection of claim 2 has not changed between the First Action and the ACP. In both, the Office and the Requester have relied on the same process, the RPC binding process, to show how the limitations of claim 2 are met. Request at 109-15; First Action at 12-13; ACP at 61-64. For example, in explaining how the elements of claim 2 were satisfied, the Office described a portion of that process—querying the CDS for a network address—that used a client server model. Patent Owner contends this is a new rejection by incorrectly asserting that it combines elements of the client server and RPC models. In reality, the querying process is part of the RPC binding process, as was explained in the Request and the First Action. "The CDS is a secure name service," and it controls access to "'[n]ames in the namespace, including clearinghouses, directories, object entries, softlinks, and child pointers.'" Request at 112-13 (quoting *Lendenmann* at 34). The Request also explained that RPC applications can post and access information on the CDS using the Name Service Interface (NSI): "'Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information.'" Request at 107 (quoting *Lendenmann* at 178-79). The Office also observed in the First Action that this information is used during the RPC binding process, "[w]here the client can utilize the namespace maintained by the CDS for the location of a server that handles the interface that the client is interested in." First Action at 12 (citing *Lendenmann* at 182). Simply put, there is nothing new about the Office's analysis, nor does it rely on a "disjointed" combination of components that are described in *Lendenmann*. Because the Office correctly found that *Lendenmann* discloses "requesting a network address associated with the secure name," "receiving a message containing the network address associated with the secure name," and "sending a message . . . using a secure communications link," the rejection of claim 2 set forth in the ACP was proper and should be maintained.

b. *Lendenmann* Discloses a "Secure Name"

Patent Owner asserts the Office has incorrectly interpreted a "secure name" in a manner inconsistent with the specification. As explained above in the discussion of the basis of the rejection of claim 1, Patent Owner's arguments rest on its belief the claims incorporate limitations shown for specific examples in the specification. The claims do not, as explained above. Moreover, Patent Owner's assertions are inconsistent with its prior representations to the Office as to what a "secure name" may constitute. Consequently, the Office correctly found that *Lendenmann* discloses a "secure name" as that term is used in claim 2.

c. *Lendenmann* Discloses a "Second Device"

Patent Owner argues that the Office has improperly "mixed and matched" various elements of *Lendenmann* to be the "second device" recited in claim 2. According to Patent Owner, the Office and the Requester have asserted that the second device is both the entire DCE cell and a particular server within the cell. Second Response at 22 (citing Request at 111-15). Patent Owner's argument is based on its own misunderstanding of the ACP and the Request. As explained above with respect to claim 1, a "first device" can be <u>either</u> the RPC server <u>or</u>, if the client and server are in different DCE cells, the DCE cell to which the RPC server belongs. Similarly, a "second device" can be <u>either</u> the RPC client <u>or</u>, if the client and server are in different DCE cells, the DCE cell to which the RPC client belongs. Accordingly, *Lendenmann* discloses a "second device" pursuant to claim 2.

d. *Lendenmann* Discloses a "Secure Name Service"

In its First Response, Patent Owner argued that *Lendenmann* does not disclose a "secure name service." First Response at 21-22. The Office responded by explaining that, based on Patent Owner's representations in the prosecution history of the '181 patent and the related '180 patent reexamination, the *Lendenmann* CDS was a "secure name service" within the broadest reasonable construction of that term.

In its Second Response, Patent Owner again argues that *Lendenmann* does not disclose a "secure name service," but now asserts that the Office's construction "contradicts" examples shown in the specification of the '181 patent. This assertion is a red herring – the only "contradiction" that exists at this point is Patent Owner's new interpretation about the '181 specification relative to its prior representations about <u>the same specification</u>. Specifically, in the its earlier representations to the Office, Patent Owner asserted the common specification of the '181 patent compelled the conclusion that a "secure name" was simply a non-standard domain name. And during original examination of the '181 patent, Patent Owner asserted the term could be a "secure name" could be "a secure non-standard domain name" or a "telephone number." First Action (Order) at 5.

There also is no "contradiction" between the Office's definition of "secure name service" and the '181 specification, as Patent Owner contends. Second Request at 23. The example Patent Owner cites from the specification falls within the scope of the Office's construction of "secure name service." Patent Owner's new opinions about the scope of this claim term is, thus, not a "contradiction" but simply a difference of opinion with the Office. If Patent Owner wishes the terms of its claims to have a different scope than what is compelled by the plain language used in those claims, it must amend the claims to correspond to that desired meaning. Because it has not done so, the Office must disregard Patent Owner's arguments that *Lendenmann* does not disclose a "secure name service."

Patent Owner's next criticism can also be dismissed. Patent Owner criticizes the Office's explanation why *Lendenmann* shows a "secure name service" by asserting that the Office has not proven that *Lendenmann* handles X.500 name resolution requests differently than how it handles DNS requests. Patent Owner misses the point – the capacity of the *Lendenmann* systems to act on X.500 names shows that those systems are a "secure name service" within the meaning of the claims. The claims require nothing more. Moreover, there is no requirement in the claims that a system that can function as a "secure name service" cannot also function as an "unsecure" name service. The contrast Patent Owner tries to make can simply be disregarded as it is irrelevant to what has been claimed.

Patent Owner also asserts again that the '181 specification shows that "the standard top-level domain name is replaced with the secure top-level domain name." Second Response at 23. Nothing in claim 2 requires the "replacement" of a "standard top-level domain name" with a "secure top-level domain name." Instead, as the Office found, the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name." Moreover, the Office's construction is consistent with Patent Owner's position during litigation, where it asserted that "Apple server(s) act as a secure name service by storing a network address (*e.g.*, an IP address) associated with the secure name of the of the second device, related to the device's email address or telephone number." Exhibit A at 17-18. The Office thus properly concluded that *Lendenmann* discloses a "secure name service" as specified by claim 2.

e. *Lendenmann* Discloses a "Sending a Message to the Network Address Associated With the Secure Name of the Second Device Using a Secure Communication Link."

The Office correctly found that *Lendenmann* discloses sending a message to the network address associated with a secure name of the second device using a secure communication link. In its Second Response, Patent Owner simply repeats argument it presented in its First Response that no "nexus" exists between security and X.500 names. In the ACP, the Office properly rejected this argument, and it can do so again without further comment. As the Office and the Request each explained, the X.500 name service shown in *Lendenmann* is inherently a secure function because it only is available within a secure network environment. Request at 103-05; ACP at 56, 58. In addition, the claims impose no specific type of connection between the secure name service and the overall functioning of the claimed systems.

Patent Owner also complains that the Office failed to address its prior arguments. This is incorrect; Patent Owner is simply unhappy that the Office found those arguments unpersuasive and did not adopt them. The Office was correct in doing so. For example, in its First Response, Patent Owner sought to read unclaimed limitations from the specification into the claims to prohibit the implementation of any security measures when an "unsecure name" was used. First Response at 39-40. The Office correctly found that the claims imposed no such limitation, and concluded that *Lendenmann* discloses exactly what the claims require: "sending a message to the network address associated with the secure name of the second device using a secure communication link." Patent Owner's attempts to read limitations from the specification into the claims should again be rejected, and the rejection of claim 2 should be maintained.

3. Dependent Claims 5 and 6

The Office correctly found that *Lendenmann* anticipates every limitation of dependent claims 5 and 6. Patent Owner responds that the encryption identified by the Office in the First

Action and ACP do not apply to the messages of claims 5 and 6. Patent Owner is wrong. As the Office found, the CDS is part of *Lendemann*'s security service and the security service provides for encrypted communication between devices. ACP at 65. Thus, *Lendenmann* discloses "receiving the message containing the network address associated with the secure name of the second device . . . in encrypted form" and "decrypting" that message. Accordingly, the Office's rejection of claims 5 and 6 was proper and should be maintained.

4. Dependent Claim 21

The Office properly found that *Lendenmann* describes a system that anticipates claim 21. In response, Patent Owner argues that the "Office's reasoning again has no bearing on the claim" and refers to the arguments made in its First Response. The Office properly disregarded those earlier arguments, as they are unpersuasive. Patent Owner also cites to its prior arguments relating to claim 2, which were unpersuasive and should be disregarded. Accordingly, the Office's rejection of this claim was proper and should be maintained.

5. Independent Claim 24 and Dependent Claim 25

The Office correctly found that *Lendenmann* describes each and every limitation of claims 24 and 25. In response, Patent Owner asserts the rejections should be withdrawn because the Office has used "the same claim interpretation . . . that plague[d] its rejections of claims 1 and 2," referring to the construction of a "secure name" and "unsecure name." Second Response at 25. The Office's interpretation of the claims is neither flawed nor has it changed during the course of the proceeding. Rather, it is the Patent Owner that seeks to improperly limit the scope of the claims by reading unclaimed limitations into them.

Patent Owner also asserts that a "non-final office action is in order" because "what the Office means by 'secure' and 'unsecured,' remain far from settled." *Id.* at 26. There is nothing unsettled about the claim construction the Office has employed – it has remained constant throughout this proceeding. This comment is simply another transparent attempt by Patent Owner to improperly delay these proceedings. As Patent Owner has offered no arguments that would rebut the Office's findings, the rejection of claims 24 and 25 was proper and should be maintained.

6. Independent Claim 26 and Dependent Claim 27

The Examiner correctly found that *Lendenmann* describes each and every limitation of claims 26 and 27. In response, Patent Owner rehashes its arguments from its First Response, asserting that *Lendenmann* does not disclose a server that has a "secure name," an "unsecure name," and a "unique network address." Response at 26-27. Again, Patent Owner's argument rests fundamentally on its desire to incorporate unclaimed limitations into the claims to avoid the prior art.

Here, the claims require registration of an "unsecured name associated with the first device" and "registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name." A device in the *Lendenmann* scheme can be registered with the CDS to be associated with a domain name and also with an X.500 name. This is all that the claims require (*i.e.*, registration with a unsecure and with a secure name). *Lendenmann* also shows that each device has a unique network address, and that the X.500 name is associated with that address. As the Office explained in the ACP, "The X.500 and domain names associated with a device in the *Lendenmann* scheme thus comprise both a unsecure and a unique secure network address. . . . [T]he whole purpose of addressing is for the locating of unique network locations, where *Lendenmann* teaches means for providing naming to network ends where the name corresponds to a specific network address." ACP at 68-69. The Office correctly found that *Lendenmann* discloses all the limitations of claims 26 and 27. Its rejection of those claims was proper and should be maintained.

7. Independent Claims 28 and 29

Patent Owner presents no arguments that are distinct from its arguments provided in response to the rejection of other claims. Because the rejections of those other claims were proper, the rejection of claims 28 and 29 based on *Lendenmann* should be maintained. *See also* Request at 147-160.

8. Dependent Claims 3-9, 12-15, and 18-23

Patent Owner presents no arguments regarding the rejection of claims 3-9, 12-15, and 18-23 based on *Lendenmann* that are distinct from the arguments it provided in response to the rejection of claim 2 over *Lendenmann*. Because the latter rejection was proper, the Examiner's rejection of claim 3-9, 12-15, and 18-23 based on *Lendenmann* is also proper and should be maintained. *See also* Request at 115-130.

F. Response to Patent Owner's Arguments Regarding the Rejection of Claims 10, 11, 16 and 17 Based on *Lendenmann* in view of *Beser* (Issue 7).

The Office properly found that *Lendenmann* in view of *Beser* describes a system that would render obvious claims 10, 11, 16, and 17. In response, Patent Owner asserts simply that *Beser* does not remedy the deficiencies of *Lendenmann*, and refers to its response to the Office's rejection of claim 2 for anticipation by *Lendenmann*. Response at 27. Because the Patent Owner presents no response to the obviousness rejection of claims 10, 11, 16, and 17, that rejection was proper and should be maintained. *See also* Request at 161-163, 164.

G. Response to Patent Owner's Arguments Regarding the Rejection of Claims 10 and 11 Based on *Lendenmann* in view of *RFC 2401* (Issue 8).

The Office properly found that *Lendenmann* in view of *RFC 2401* describes a system that would render obvious claims 10 and 11. In response, Patent Owner asserts only that *RFC 2401* does not remedy the deficiencies of *Lendenmann*, and refers to its response to the Office's rejection of claim 2 for anticipation by *Lendenmann*. Response at 27. Because Patent Owner presents no response to the obviousness rejection of claims 10 and 11, that rejection was proper and should be maintained. *See also* Request at 164-166.

H. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-23 and 28-29 Based on *Provino* (Issue 9).

1. The Office's Rejection of *Provino* Has Remained Consistent

Patent Owner first contends that the Office has "adopted a new rejection" in the ACP. Second Response at 28. Patent Owner's theory is incorrect. Patent Owner omits its assertions in the First Response, which prompted the response of the Office regarding the teachings of Provino. In reality, the manner in which the Request, the First Office Action and the ACP each refer to the disclosure of a "secure name" in *Provino* has remained consistent. For example, the Request, which was incorporated into both the First Office Action and the ACP, explained:

> Provino explains that these DNS systems include secure nameservers (*e.g.*, Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.

Request at 170 (citing *Provino* at 8:67-9:5). Patent Owner ignored this observation in its First Response. This passage shows that a domain name acted on by Nameserver 32 (and which is resolvable into an IP address, *i.e.*, an "integer Internet address") comprises a "secure name" as specified in the '181 patent claims. Thus, the Office has not changed its position on what Provino teaches, much less changed the statutory or substantive basis of the rejections imposed over Provino.. Instead, it has maintained the same rejection that was previously imposed. *See, e.g.,* Request at 168-171; ACP at 71-73. Patent Owner thus is simply incorrect..

2. Independent Claim 1

In the ACP, the Office correctly maintained its determination that *Provino* anticipates claim 1. In response, Patent Owner asserts the rejection "does not clearly identify the 'First Device' and 'Second Device" of the claim, and that *Provino* does not disclose "a network address corresponding to the secure name associated with the first device," does not disclose the claimed "unsecured name" and is "essentially a Firewall-Based System like those disparaged and disclaimed in the '181 Patent Specification." Second Response at 28-30. Each of these assertions is incorrect, and should be disregarded.

a. Each Rejection Clearly Identifies the First and Second Devices

Patent Owner first asserts that the Request "mixed and matched features from two different devices" in *Provino*, and that Requester has changed its position on which features of *Provino* anticipate the claims. The criticisms levied by Patent Owner are unfounded – Requester's position is unchanged. For example, the Request and First Office Action both pointed out that server 31(S) is the claimed "first device" and "device 12(m)" is the claimed second device in *Provino*. *See, e.g.,* Request at 168-71; First Action at 15-17. Patent Owner's criticisms are simply baseless.

b. Provino Discloses "a Network Address Corresponding to the Secure Name Associated With the First Device"

Patent Owner mischaracterizes the Office's statements regarding "a network address corresponding to the secure name associated with the first device" limitation. Specifically, Patent Owner again incorrectly asserts the Office "now contends that the claimed 'secure name' is 'the integer Internet address' registered with the VPN server of Provino." Second Response at 28-30. This is simply incorrect. As noted above, the Office has consistently explained that the domain names in nameserver 32 of *Provino* constitute the "secure name(s)" disclosed in the '181 patent claims. Thus, as explained in the Request (at 174-175, for example) and the ACP (at 71-73), the "integer Internet address," which is resolvable from the domain name, is the "network address corresponding to the secure name associated with the first device." Patent Owner also contends reading *Provino* in this manner "effectively reads" clauses out of the claims. Petant Owner's assertion rests on its incorrect portrayal of the basis of the rejection and what is shown in *Provino*. It also mischaracterizes the claims, which do not foreclose an integer network address from serving as both the "secure name" and the "network address corresponding to the secure name." Patent Owner's comments, thus, are incorrect and irrelevant to the claims.

c. Provino Discloses an "Unsecured Name"

Patent Owner again contends that *Provino* does not disclose a method for "communicating with a device associated with a secure and an unsecured name…" by asserting the claims exclude the system being described in *Provino*. In particular, Patent Owner claims that nameserver 17 <u>alone</u> "…will not contain any names or addresses associated with [secure nameserver 31(S).." and that "the device 12(m) … will not be able to obtain the integer Internet address of server 31(S) which is accessed from that nameserver 17." Second Response at 29. Patent Owner's comments again incorrectly describe the *Provino* systems and ignores the claim language. <u>First</u>, the <u>claims</u> do not restrict a "device" to a single component shown in the *Provino* systems considered in isolation. Instead, as explained in the Request and the prior actions from the Office, the Provino devices comprise multiple components that interact with each other to provide the functionality specified by the claims. Request at 167-72; First Action at 15-17; ACP at 69-74. Thus, the claims do not require one component in Provino to perform all the functions specified in the claim. <u>Second</u>, in the '181 disclosure, Patent Owner identifies multiple discrete components that interact with each other to provide specified functionalities. *See, e.g.*, Fig. 26 showing DNS server 2609 and DNS Proxy 2610 interacting with "Gate Keeper" 2603 to handle and resolve secure vs. unsecure names. The Office, thus, correctly refuted Patent Owner's incorrect contentions about the capacities and functions of the *Provino* system. *See* ACP at 71-72. Because it has not proposed to amend its claims to exclude the embodiments shown in *Provino,* Patent Owner's arguments must be disregarded.

d. The *Provino* System is Within the Meaning of the Claims of the '181 Patent.

Patent Owner next criticizes the *Provino* scheme, asserting it consists simply of "placing a conventional domain name server behind a firewall" and that this does not "convert it from being conventional into a secure domain name server." Second Response at 30. Patent Owner adds that "a secure domain name server must possess additional functionality not present in a conventional domain name server…" *Id.* Patent Owner concludes that because it "disparaged" conventional domain name servers during prosecution of the '181 patent, the "claims cannot be read to encompass those systems." *Id.* (also citing pages 45-46).

Patent Owner again mischaracterizes both what *Provino* teaches and what its claims encompass. First, *Provino* does not, as Patent Owner contends, consist simply of a conventional name server behind a firewall. Instead, as previously explained, *Provino* shows a system comprising multiple components that work together to receive, at a network address corresponding to a secure name associated with a destination device (*e.g.*, firewall 30, VPN name server 32) a message from a second device to securely communicate. *See*, *e.g.*, *Provino* at Fig. 1. The routing of a request to that destination where it is evaluated and acted upon is part of the *Provino* system, which means the message will also be received, *inter alia*, by device 12(m) and Name Server 17. If the request specifies a desire to "securely communicate" (*e.g.*, by requesting access to a secure resource within VPN 15 in *Provino*), and the user's credentials are valid, then a VPN is established, and a message (*e.g.*, data for the requested resource) is sent to the requesting entity (the "second device" in claim 1). Moreover, explained in the Request and ACP, the VPN Server 32 is not accessible in the same manner as a conventional domain server. Instead, the *Provino* VPN Server 32 facilitates a secure communication link with authorized devices in the same manner as the "secure name service" described in the '181 patent. Thus, far from being "disparaged and disclaimed," the disclosure of VPN Server 32 in *Provino* is no different than the "secure name service" described by Patent Owner. *Provino*, thus, plainly shows everything required by the claim 1, and therefore anticipates this claim.

Second, the unspecified "additional functionality" Patent Owner refers to is neither identified by it nor is it actually claimed. Instead, the claims by their literal terms encompass the exact systems described in *Provino.* Requester again observes that Patent Owner's "disparagement" theory is factually incorrect and legally irrelevant in this proceeding. For example, the original prosecution history does not show that Patent Owner "disparaged" secure domain name servers such as those shown in *Provino*. In fact, the secure name servers in the '181 specification mirror precisely the *Provino* scheme. In addition, even if Patent Owner had made an effective disclaimer of certain subject matter – which it plainly does not – that disclaimer would only be relevant if it was accompanied by amendment to the claim language that made the claims correspond to that proposed meaning. Since it has not amended the claims, its "disparagement" arguments are legally irrelevant.

3. Independent Claim 2

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of independent claim 2. ACP at 74. In response, Patent Owner presents no response for claim 2 distinct from its response to the rejection of claim 1 over *Provino*. Because the rejection of claim 1 over *Provino* was proper, the Office's rejection of claim 2 over *Provino* also was proper and should be maintained.

4. Claims 3-15, 18-23, and 28-29

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 3-15, 18-23, and 28-29. ACP at 74-75. In response, Patent Owner presents no response for claims 3-15, 18-23 and 28-19 distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 3-15, 18-23, and 28-29 over *Provino* also was proper and should be maintained.

5. Dependent Claim 23

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 23. ACP at 75. In response, Patent Owner presents no response distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 23 over *Provino* also was proper and should be maintained.

6. Independent Claim 28

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 28. ACP at 75. In response, Patent Owner presents no response distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 28 over *Provino* also was proper and should be maintained.

7. Independent Claim 29

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 28. ACP at 75. In response, Patent Owner presents no response distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 1 over on *Provino* also was proper and should be maintained.

I. Response to Patent Owner's Arguments Regarding the Rejection of Claims 24-26 Based on *Provino* in view of *H.323* (Issue 10).

Patent Owner contests the rejection of claims 24-26 as being obvious over *Provino* considered in view of *H.323* without presenting substantive objections to the teachings of either reference. Instead, Patent Owner (i) asserts the Office changed its interpretation of the teachings of *Provino* and this makes it difficult to understand the basis of the rejection, and (ii) disputes that the H.323 properly "incorporates" the teachings of the H.235 publication. Second Response at 31. Neither assertion has any legitimate basis, and each should be disregarded.

First, the basis for the rejection was clearly explained in the Request and the First Action, and has not changed in the ACP. *See* Request at 188-201; First Action at 18; ACP at 75. Patent Owner's assertion that the Office has changed its interpretation of *Provino* and the rejected claims, thus, is incorrect. *See* §H above *Provino*.

Second, the Office properly rejected Patent Owner's "improper incorporation by reference" theory regarding the teachings of *H.323* and *H.235*. *See* ACP at 75-76. As the Office pointed out, *H.323* expressly incorporates *H.235* as "constituting provisions of this [*i.e.*, the *H.323*] Recommendation" (*see* Request at 204 (citing *H.323* at 2-3)) and by stating that "[A]uthentication and security . . . if it is provided, it shall be provided in accordance with Recommendation H.235. Request at 206 (citing *H.323* at 81) (emphasis added). *See also* ACP at 76 ("The Examiner agrees with the third party Requester, H235 is being reference as a standard for security and encryption of H-Series multimedia terminals").

Patent Owner then asserts that it "is not clear how the Office contends the claims are obvious over *Provino* in combination with *H.323* by itself or also in combination with *H.323*." The basis for the rejection of these claims 24-26 is clearly explained in the Request, the First Action and the ACP. Request at 188-201; First Action at 18; ACP at 75. As Patent Owner presents no response specific to the combination of *Provino* with *H.323*, there is no basis for the Office to withdraw its previously imposed rejections, which should be maintained.

J. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-29 Based on *H.323* (Issue 11).

1. Independent Claim 1

In the ACP, the Office maintained its determination that *H.323* describes a system that anticipates claim 1. In response, Patent Owner asserts the same arguments it presented in its First Response, namely that "[c]ombining the teachings of *H.323, H.245, H.235*, and *H.225* is improper," and that *H.323* does not disclose (1) "[a] first device associated with a secure name and an unsecured name," (2) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, and (3) "sending a message over a secure communication link from the First Device to the Second Device." Second Response at 32-40. These arguments do not materially change the arguments the Office previously found unpersuasive, and rest on incorrect characterizations of *H.323* and its incorporated teachings.

a. The Teachings of *H.323, H.245, H.235*, and *H.225* Are Properly Combined

In the First Office Action and the ACP, the Office correctly found that *H.245, H235* and *H.225* were expressly incorporated into the disclosure of *H.323*, which anticipates claim 1. In its Second Response, Patent Owner again asserts that *H.323* does not properly incorporate the teachings of *H.323, H.245, H.235,* and *H.225* because *H.323* "does not identify with detailed particularity the subject matter" of those references. Second Response at 32-22. Patent Owner is, again, incorrect. First, as explained in the Request, *H.323* expressly incorporates *H.245, H.235,* and *H.245* as "constituting provisions of this [*i.e.*, the *H.323*] Recommendation." Request at 204 (citing *H.323* at 2-3). That is sufficient to incorporate the teachings of *H.245, H.235*, and *H.225* in their entirety. *See Harari v. Lee*, 656 F.3d 1331, 1335 (Fed. Cir. 2011) (holding "broad and unequivocal" language sufficient to incorporate the entire disclosure of another reference). Even under stricter standard proposed by Patent Owner, each of *H.245, H.235*, and *H.245* was properly incorporated by reference. For example, *H.323* explains that "authentication and security for H.323 is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235." Request at 204-05 (citing *H.323* at 81 (emphasis added)). Similarly, *H.323* discloses that products claiming compliance with Version 2 of *H.323* shall comply with all of the mandatory requirements of H.323 (1998) which references Recommendations H.225[] (1998) and H.245 (1998)." Request at 205 (citing *H.323* at (i) (emphasis added)). *H.323* also describes *H.225* as containing "[c]all signaling protocols and media stream packetization for packet based multimedia communication systems," and *H.245* as containing "[c]ontrol protocol for multimedia communication." Request at 206-08 (citing *H.323* at 2-3). Each of these statements was identified in the Request, the First Office Action, Requester's comments, and the ACP. Patent Owner continues to ignore these statements in its latest response. Because *H.323* incorporates by reference the teachings of *H.225, H.235*, and *H.245*, the Office's rejection was proper and should be maintained.

Patent Owner also generally argues that, even if the references were properly combined, the Office has "mixed and matched" features from multiple embodiments in *H.323*. Second Response at 31-32. These belated comments should be disregarded as they are not timely. In addition, they should be rejected because Patent Owner does not identify any specific features of *H.323* that were improperly combined. Were the Office to even consider Patent Owner's vague objection, it would be left to guess at which features Patent Owner believes were improperly combined. Finally, Patent Owner's assertions are premised on the mistaken belief that the IPsec protocol cannot be used when an endpoint is protected by a security token. Indeed, *H.323* clearly shows that IPsec is used with security tokens and that IPsec and tokens are part of the same embodiment. Request at 218-26. Because the Office correctly found that *H.323* incorporates the teachings of *H.225, H.235*, and *H.245*, the rejection of the claims over *H.323* were proper and should be maintained.

b. *H.323* Discloses "A First Device Associated With A Secure Name and An Unsecured Name"

The Office correctly determined that *H.323* discloses "a first device associated with a secure name and an unsecured name." ACP at 79-80. In response, Patent Owner again contends that *H.323* does not describe a first device associated with both a "secure name" and an "unsecured name." Second Response at 34-35; First Response at 54. Patent Owner also asserts the Office adopted a new basis for its rejection in the ACP. For the reasons the Office has already conveyed and as set forth below, Patent Owner's contention are incorrect.

First, Patent Owner incorrectly asserts the Office relied on access tokens and the URL of a gatekeeper to satisfy the secure and unsecured names in the First Action, but that in the ACP, relied on "that a 'name and address linked via a registry' correspond to the secure name and unsecure name." Second Response at 34. Patent Owner misunderstands the *H.323* disclosure and the ACP. The ACP did not set forth a new basis for the rejection – the passage referenced by Patent Owner merely refers to a different part of the process described in *H.323* that was identified in the Request and the First Action. Specifically, the Request and the ACP explain that *H.323* discloses that each device in an *H.323* network "is associated with one or more alias names, called Alias addresses, which can be in the form of a phone number or an email address." ACP at 79 (quoting Request at 204). Alias addresses are "secure," in part, because they are "protected by 'access tokens,' which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses." ACP at 79 (quoting Request at 204). The Request also explained that a device will "be[] associated with the unsecured names of the Gatekeeper computer with which they are registered," (Request at 210), and will also "register[] an Access Token instead of a regular Alias address with the Gatekeeper to secure its name and to receive communications at the network address associated with the secure name," (Request at 213).

Patent Owner also complains about the Office's construction of a "secure name" and "secure name registry." Patent Owner's complaint is that the Office has not limited these terms to the examples shown in the specification, or that the Office has disregarded arguments Patent Owner previously made. Patent Owner's criticisms are baseless. Under the Office's broadest reasonable construction policy, a patent owner must amend the claim language to effectively exclude from its scope subject matter literally encompassed by that claim language. *See, e.g.*, M.P.E.P. § 2111.

Requester also notes the Office's construction of these terms as reading on the use of an access token to protect an alias in *H.323* is consistent with Patent Owner's own application of a "secure name" in concurrent litigation against the Requester. In that litigation, Patent Owner contended that Apple's FaceTime "server(s) rely upon a local security certificate on the first Accused Device to secure the name of that device." Exhibit A at 2; *accord id.* at 4. Patent Owner cannot have it both ways. Accordingly, the Office properly determined that *H.323* discloses "a first device associated with a secure name and an unsecured name."

c. *H.323* Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"

In the ACP, the Office correctly maintained its finding that *H.323* discloses the above claim requirement. ACP at 80-84. In response, Patent Owner offers no new arguments, but simply repeats its baseless assertions regarding the Office's supposed "token-based arguments" and "IPSEC-based rejections." Second Response at 35-39. The Office properly rejected those assertions before, and should do so again. Moreover, Patent Owner mischaracterizes the ACP –

the Office did not impose independent token-based and IPsec-based rejections. As explained above, IPsec is an optional feature that can be implemented along with security tokens. *See* Request at 218-26.

In its challenge to the so-called "token-based" rejections, Patent Owner asserts that none of the devices and messages disclosed in *H.323* corresponds to the "message" or "device[s]" of the claims. Spefically, Patent Owner argues that "[n]one of these messages is sent from the alleged second device (Endpoint A) and 'received, at a network address corresponding to the secure name associated with' the alleged first device (POTS-B). . . . Rather, POTS-B does not receive any message at all in the disclosure of H.235 . . . ." Second Response at 36. Patent Owner's assertions should be disregarded, as the claim language specifies simply that the message be "receiv[ed], at a network address corresponding to the secure name associated with the first device." Patent Owner's argument is thus premised on its mistaken belief that the claims require the message requesting a secure communication link to be received by the first device itself rather than "at a network address corresponding to the secure name associated with the first device." Nothing in the claim language precludes establishment of the secure connection from being mediated by intermediary devices.

Patent Owner's next contention is similarly flawed. Specifically, Patent Owner asserts that the second device does not send a request to securely communicate directly to the first device because the gateway protects that device's addressing information with an access token. Second Response at 36-37. But that assertion is premised on an improper characterization of what the claims actually encompass and ignores that the Office already determined that it is not inconsistent with the claim language for "the gateway [to] act[] and [sic] an intermediary to control access" or for the gateway to "obscure or hide destination addressing information." ACP at 81, 83. This assertion by Patent Owner may therefore be readily dismissed.

Patent Owner's challenge to the purported "IPSec-based" rejections suffer from the same flaws. Here, Patent Owner asserts the messages are "either sent from an endpoint to a gateway, or from a gatekeeper to an endpoint—not from the alleged second device to the first device, as required by the claim." Second Response at 38. Once again, the claim language provides only that the message be "receiv[ed], at a network address corresponding to the secure name associated with the first device." The Office properly concluded that the secure connection can be mediated by intermediary devices. ACP at 81, 83. *See also* Request at 215-16; ACP at 82-83 (explaining that calling endpoint establishes a channel with the receiving endpoint via a gatekeeper, and the endpoints can negotiate a secure channel either during setup or after the connection has been established). Patent Owner's criticisms can thus be ignored, and the Office should maintain its finding that *H.323* discloses this limitation.

d. *H.323* Discloses "Sending a Message over a Secure Communication Link from the First Device to the Second Device."

The Office correctly maintained its determination that *H.323* discloses "sending a message over a secure communication link from the first device to the second device." ACP at 80-84. In response, Patent Owner argues only that the Office failed to address its arguments in the First Response. Patent Owner is again incorrect. In its prior response, Patent Owner asserted that *H.323* did not show a secure communication link between endpoints. This argument rests on the same, incorrect belief that intermediary devices could not broker a secure communication link. First Response at 58-59. The Office properly rejected that assertion by referring to the actual claim language, and noted Patent Owner had offered no new arguments with respect to the "sending" limitation. ACP 81-84. Consequently, the Office fully addressed and rejected Patent Owner's assertions. The rejection of claim 1 was thus proper and should be maintained.

2. Independent Claim 2

In the ACP, the Office correctly maintained its determination that *H.323* anticipates every limitation of independent claim 2. ACP at 84. In response, Patent Owner repeats the arguments from its First Action, namely that *H.323* fails to disclose (1) "a secure name"; (2) "a network address associated with the secure name of the second device"; (3) "'from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device' and 'at the first device, receiving a message containing the network address associated with the secure name of the second device'"; and (4) "'from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.'" Second Response at 40-44. For the reasons the Office has already conveyed, each of these contentions is incorrect.

a. *H.323* Discloses "A Secure Name"

The Office correctly maintained its determination that *H.323* discloses "a secure name."

In response, Patent Owner presents no response distinct from its response to the rejection of claim 1 over *H.323*. ACP at 84. Because the Office's rejection of claim 1 was proper, its determination that *H.323* discloses the "secure name" of claim 2 was also proper. *See* ACP at 79-80, 84; *see also* Request at 218-226.

b. *H.323* Discloses "A Network Address Associated with the Secure Name of the Second Device"

In the ACP, the Office correctly maintained its determination that *H.323* discloses "a network address associated with the secure name of the second device." ACP at 85-88. In response, Patent Owner repeated its argument that *H.323* does not disclose "a network address associated with the secure name of the second device." Patent Owner's assertion is premised on unclaimed limitations of the claims that would exclude intermediary devices from assisting with establishing a secure connection. The Office properly rejected Patent Owner's assertions when presented previously, and should do so again. ACP at 84-85. The claim language provides only that the "network address" be "associated with the secure name of the second device" and, as the Office found, Patent Owner "attempts to read non-existent limitations into the term 'associated.'" ACP at 86. In the ACP, the Office properly concluded that "the gatekeeper acts and [sic] an intermediary to control access" and "the address of the gateway associated with the second device is sufficient to read on the claim." ACP at 85-86. Accordingly, the Office should maintain its finding that that *H.323* discloses the above limitation.

c. *H.323* Discloses a "'From the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated With the Secure Name of the Second Device' and 'at the First Device, Receiving a Message Containing the Network Address Associated With the Secure Name of the Second Device'"

In the ACP, the Office correctly maintained its determination that *H.323* discloses the above claim requirements. ACP at 85-88. In response, Patent Owner simply repeats the same assertions it made in its First Response. The crux of Patent Owner's position again rests on unclaimed limitations and features of the claims that would prohibit intermediary devices from assisting with establishing a secure connection. For example, Patent Owner asserts that the Office's construction "incorrectly incorporates . . . into the claim . . . [a] third device: the Gateway." Second Response at 42. Similarly, Patent Owner also contends that the security token embodiment cannot read on the claims because "POTS-B has shielded its alleged 'secure name'—the E.164 phone number—from Endpoint A with the security token," and thus, Endpoint A cannot "request[] a name associated with POTS-B's E.164 phone number." Second Response at 42. But the Office has consistently and properly rejected those arguments, explaining that the use of intermediary devices falls within the broadest reasonable construction of the claims. ACP at 85 ("the gateway acts as an intermediary to control access"). Patent Owner also alleges that the Office "pick[s] and choose[s]" features from various unrelated embodiments to satisfy the claims. That assertion rests on the same, incorrect belief that the claims exclude intermediary devices, and therefore the gateway must be considered a first or second device.

d. *H.323* Discloses "From the First Device, Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

In the ACP, the Office correctly found that *H.323* discloses "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." ACP at 87-88. In response, Patent Owner presents no response distinct from its response to the rejection of claim 1 over *H.323*. Because the Office's rejection of claims 1 was proper, its determination that *H.323* discloses the above limitation of claim 2 also was proper. *See also* Request at 224.

3. Dependent Claims 3-23

In the ACP, the Office correctly found that *H.323* discloses each and every limitation of dependent claims 3-23. ACP at 88. In response, Patent Owner presents no response distinct from its response to the rejection of claims 1 and 2 over *H.323*. Because the rejection of claims 1 and 2 was proper, the Office's rejection of claims 3-23 based on *H.323* also was proper and should be maintained. *See also* Request at 226-242.

4. Dependent Claim 4

In the ACP, the Office correctly maintained its determination that *H.323* anticipates every limitation of dependent claim 4, which provides "the method according to claim 2, wherein the secure name indicates security." ACP at 88. As it did in response to the First Action, Patent Owner contends that the Office "improperly mixed and matched various distinct components of various different references in attempting to meet the claim language." Second Response at 44-

45; *see* First Response at 63. Patent Owner is still incorrect; the only way it can assert that the Office has mixed and matched components is, as explained above for claims 1 and 2, by ignoring the disclosure of *H.323* and misconstring what the claims actually encompass.

Patent Owner also incorrectly asserts that the Requester took a "new position" in its Comments by asserting that the "access token" can satisfy the "wherein the secure name indicate security" limitation of claim 4. Second Response at 44. But the use of the access token was clearly identified in the Request and, in fact, Patent Owner addressed this access token in its own First Response. First Response at 63; Request at 220-23 (explaining how a gatekeeper will recognize the addresses and aliases associated with an access token, "as a 'private' alias, knowing that in order to complete the connection it must return the POTS-gateway address "). Similarly, Patent Owner incorrectly contends that the Office took a new position in the ACP that a "generic name"—a "phone number" or "email address"—corresponds to a secure name. The Office's position is neither new nor different from Requester's. In the ACP, the Office explained that the address of the device corresponding to such an email address or phone number could be protected by an access token. ACP at 79-80. It also found that "access tokens, which obfuscate the destination address information, thus indicate security.'" ACP at 88. The Office's and the Requester's positions are not new, and the Office previously conveyed how the limitations of claim 4 are anticipated by *H.323*. Patent Owner's contentions are simply incorrect.

5. Dependent Claim 5

In the ACP, the Office correctly determined that *H.323* anticipates every limitation of dependent claim 5. ACP at 89. In response to the First Action, Patent Owner argued that *H.323* "fail[s] to disclose 'receiving a message containing the network address associated with the secure name of the second device,' as received in claim 2. For the additional claim 5 feature . . . the address returned in the IPsec passage corresponds to a 'call signaling channel,' rather than the endpoint earlier identified as the 'second device . . . .'" First Response at 63. In the ACP, the Office rejected that argument, observing that Patent Owner had improperly imported <u>unclaimed</u> limitations into claim 2 prohibiting the use of intermediary devices. ACP at 84-85, 89. In its Second Response, Patent Owner presents the same arguments. Because they continue to be based on unclaimed limitations and features of the claims, they should continue to be rejected. In addition, Patent Owner argues the Office has failed to address its arguments relating to the "IPsec embodiment." But, as explained above under claim 2, this argument is based on

Patent Owner's misunderstanding of the H-series processes; IPsec is not a separate embodiment, but an optional feature that can be implemented to work with the security tokens of *H.323*. Accordingly, the Office's rejection of claim 5 over *H.323* was proper and should be maintained.

6. Dependent Claim 9

In the ACP, the Office correctly found that *H.323* anticipates dependent claim 9. ACP at 89-90. In its First Response, Patent Owner asserted simply that "Requester makes the conclusory assertion that any alleged communication link would be initiated automatically." First Response at 64. In response to the ACP, Patent Owner now expands on its assertions, arguing that the literal absence of the words "automatically initiating" in *H.323* means that a secure communication link established would not occur automatically upon completion of negotiation process between networked devices. Second Response at 46. Patent Owner's argument adds nothing new to its previous position, and the Office can reject it on the same basis as it did previously. Patent Owner also incorrectly describes *H.323*. As explained in the Request, First Comments, and ACP, *H.323* explains that "[a]fter obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair." Request at 219. The Office correctly determined these steps occur automatically without any further user interaction. ACP at 90. Accordingly, *H.323* discloses the limitations of claim 9, and the Office's rejection of claim 9 was proper and should be maintained.

7. Dependent Claim 10 and 11

In the ACP, the Office correctly found that *H.323* discloses each of the limitations of claims 10 and 11. ACP at 90. Claim 10 includes the requirement of "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 includes the requirement of "receiving the message in the form of at least one tunneled packet." In response, Patent Owner asserts simply that because it believes *H.323* does not anticipate claim 2, it also fails to anticipate claims dependent from claim 2. As demonstrated above, this assertion is incorrect because claim 2 does not exclude intermediary devices from brokering the secure connection. Consequently, the rejection of claims 10 and 11 was also proper and should be maintained.

8. Dependent Claim 13

In the ACP, the Office correctly found that *H.323* discloses every limitation of claim 13, which specifies that the "receiving and sending of messages through the secure communication link includes multiple sessions." ACP at 91. In its Second Response, Patent Owner makes the same argument it made in its First Response, namely that *H.323* employs separate channels and separate sessions and that claim 13 includes one secure communication link and separate sessions. Second Response at 47; First Response at 64. In the ACP, the Office found that *H.323* provided for the use of multiple sessions and that nothing in the claims limited the multiple sessions to the same secure communication link. ACP at 92. The Office correctly disregarded Patent Owner's incorrect assertions. Accordingly, the rejection was proper and should be maintained.

9. Dependent Claim 21

In the ACP, the Office correctly found that *H.323* anticipates every limitation of dependent claim 21. ACP at 92. In response, Patent Owner presents no response distinct from its response to the rejection of claim 1 over *H.323*. Because the rejection of claim 1 was proper, the Office's rejection of claim 21 based on *H.323* also was proper. *See also* Request at 237-241.

10. Independent Claims 24 and 28 and Dependent Claims 25 and 29

In the ACP, the Office correctly found that *H.323* anticipates every limitation of claims 24, 25, 28, and 29. ACP at 92-93. In response, Patent Owner presents no response distinct from its response to the rejection of claims 1 and 2 over *H.323*. Because the rejection of claims 1 and 2 was proper, the Office's rejection of claims 24, 25, 28, and 29 based on *H.323* also was proper. *See also* Request at 242-48, 258-68.

11. Independent Claim 26 and Dependent Claim 27

In the ACP, the Office correctly maintained its determination that *H.323* anticipates each and every limitation of claims 26 and 27. ACP at 92. In response to the First Action, Patent Owner presented no response distinct from its response to the rejection of claims 1 and 2. In response to the ACP, Patent Owner now complains that the Office did not respond to its argument that *H.323* does not disclose a "unique network address" as required by the claims. Patent Owner is wrong. In confirming the rejections of claims 1 and 2, the Office gave an in-depth explanation of how *H.323* anticipates the claims. ACP at 79-88. In particular, it explained how a gatekeeper in the *H.323* scheme could be associated with one device and how a device could register one secure name and one unsecured name with the gatekeeper, thus satisfying the "unique network address correspond[ing] to the secure name associated with the first device" element of the limitations. ACP at 81-83. The Office's findings also are consistent with Patent Owner's reading of a "unique network address" in concurrent litigation, in which, Patent Owner has asserted "[a] prospective FaceTime caller must also request and obtain registration of a secure name associated with the caller's device through the FaceTime system. . . . [A] certificate assures that the name of the caller's (first) Accused Device is secure. This secure name corresponds to the unique network address of the caller's (first) Accused Device. . . . To call someone using FaceTime, you need their phone number or email address. Exhibit A at 14-15. Thus, because Patent Owner has maintained that an email address or phone number secured by a certificate can "correspond to the unique network address" associated with the first device, its arguments to the contrary should be given no weight by the Office. The Office correctly addressed and dismissed each of Patent Owner's unpersuasive arguments. Accordingly, the Office's rejection of claims 26 and 27 was proper and should be maintained.

K. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-29 Based on *Johnson* in view of *RFC 2131, RFC 1034,* and *RFC 2401* (Issue 13).

1. Independent Claim 1

The Office correctly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claim 1. In response to the ACP, Patent Owner repeats and expands upon arguments it made in its First Response, namely that the references do not teach a system that discloses both "a first device associated with a secure name and an unsecured name." Second Response at 48-52. These arguments can be rejected because they are effectively the same as the arguments in Patent Owner's previous response, which the Office already considered and rejected. Moreover, the arguments are inconsistent with Patent Owner's srepresentations before the Patent Office and should be rejected for that reason.

a. Johnson in view of RFC 2131, RFC 1034 and RFC 2401 Discloses a "a Secure Name" and "a Secure Name Service"

In response to the ACP, Patent Owner states that "the term 'secure name' refers to those names used to communicate securely that are resolved by a secure name service, consistent with its statements during prosecution." Second Response at 49. However, it repeats its arguments that embodiments in the '181 specification additionally require a "secure name server" to "further support establishing a secure communications link" and that *Johnson* discloses a conventional name server that does not. Second Response at 49; First Response at 68. The Office correctly rejected this argument in the ACP, observing that *Johnson*'s secure name server implements security features that make it distinct from a conventional name server. ACP at 95. Also, in the First Action, the Office found that the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name" to distinguish it from a conventional name server. Order at 5. The Office properly rejected Patent Owner's contentions that the claims should be read as implicitly requiring more, in part because those statements are inconsistent with Patent Owner's prior representations to the Office. ACP at 94-95.

Patent Owner also repeats the argument from its First Response that *Johnson* does not disclose a "secure name," asserting that the name used to access *Johnson*'s secure mail server cannot be secure because users know the name in advance. The Office properly addressed and rejected that argument in the ACP, explaining that "the user at the first device requests access to the secure mail server via a 'name' (secure) then when they are authenticated via the secure name service, they are provided with the 'address' (unsecure) corresponding to the provided 'name.'" ACP at 96, 98. The Office correctly observed that the secure name server can require authentication before returning the corresponding network address and the mail server's name can only be resolved by the secure name server; thus the server's name is a "secure name" within the meaning of the claims. The Office thus properly confirmed that *Johnson* discloses the above listed features of claim 1.

b. Johnson in view of RFC 2131, RFC 1034 and RFC 2401 Discloses a "an Unsecured Name"

In response to the ACP, Patent Owner repeats its argument that *Johnson* in view of the other references does not disclose an "unsecured name" because it does not have a domain name registered with the public DNS system. Once again, Patent Owner is wrong. As the Request explained, *Johnson* discloses that the secure name server may be used in many applications, *e.g.*, interbusiness network communication, and it would have been obvious and necessary to register the secure name server with the public DNS system to enable such communications. Request at 272-74. Patent Owner also argues (incorrectly) that the Office changed its position in the ACP to "additionally contend[] that the dynamic address of the secure mail server in Johnson alone corresponds to the 'unsecured name.'" Second Response at 50. The Office has not changed its position. The Request, which the Office incorporated by reference, explained that "the name of the secure mail server is a secure name" and it "has its own unique IP address" as well as "a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an 'unsecured name.'" Request at 274. The Request clearly identified the mail server's address as an unsecured name. Patent Owner's contention this is somehow "new" is thus false. Patent Owner also contends that "an 'Internet protocol address' [is] not a 'name' at all." Second Response at 50. That contention should be disregarded as being inconsistent with Patent Owner's prior representations that distinguish a "secure name" from a conventional name. An IP address, especially one associated with a registered domain name, is a conventional name and it is publicly accessible.

Patent Owner also argues that *Johnson* teaches away from RFC 2131 because *Johnson* "does not rely on any of the[] methods [described in RFC 2131] to assign a dynamic address to the secure mail server." Patent Owner's argument is based on a misreading of *Johnson*. *Johnson* explains "the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network." While Patent Owner contends this teaches away from using DHCP, in fact it does not. Instead, *Johnson* discloses that when the mail server connects to the network, the network assigns it a dynamic address – that is exactly how DHCP works. The Office may thus disregard Patent Owner's contention that "Johnson identifies no DHCP server to convey the address to the secure mail server from the network." Second Response at 51.

Finally, Patent Owner argues that *Johnson*'s intention is to "limit access for security purposes" and it would make little sense for servers of Johnson to register domain names in the public DNS to expand access. However, Patent Owner fails to explain how these purposes are "diametrically opposed" since one of ordinary skill would have appreciated Johnson's intention of developing a flexible system, capable of providing secure communications both within a network and across networks via public resources such as the Internet. The combination does not compromise security or the intended purpose of *Johnson*. Accordingly, the Office properly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claim 1.

2. Independent Claim 2

The Office correctly determined that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious dependent claim 2. Patent Owner presents no response from to its response to claim 1. Accordingly, because its rejection of claim 1 was proper, the Office's rejection of claim 2 also was proper and should be maintained. *See also* Request at 276-282.

3. Dependent Claims 4-6, 8, 12 and 17-20

In the ACP, the Office correctly maintained its determination that *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claims 4-6, 8, 12 and 17-20. In response, Patent Owner presents no response distinct from its response to the rejections of claims 1 and 2. Because the rejections of those claims were proper, the Office's rejections of claims 4-6, 8, 12, and 17-20 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* also were proper and should be maintained. *See also* Request at 284-286, 287-289, 291-292, 294-297.

4. Dependent Claim 3

In the ACP, the Office correctly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered obvious dependent claim 3. In its response to the First Action, Patent Owner asserted that *Johnson* in view of *RFC 1034* failed to disclose an authoritative name server. The Office correctly rejected this argument in the ACP. ACP at 101-02. Now, in response to the ACP, Patent Owner belatedly asserts that *Johnson* in view of *RFC 1034* "does not somehow produce a 'secure domain name'." Second Response at 52-53. The Office should disregard this comment as it is untimely presented. Even if considered, it should be disregarded as being unpersuasive. As the Request explained, a person of ordinary skill in the art would have found motivation within *Johnson* to incorporate mechanisms to facilitate inter-business communications by, for example, making it possible to locate the secure name server 14 by name through the public resources of the Internet. Patent Owner's new argument is based on its misconception that *Johnson* does not show a "secure name" and an "unsecured" name which, as explained above. *See also* Request at 273-74, 282-84. Consequently, the Office's rejection of claim 3 as obvious over *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

5. Dependent Claims 9-11 and 13-16

The Office correctly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* rendered obvious dependent claims 9-11 and 13-16. In response, Patent Owner presents the same argument the Office rejected in the ACP; namely, that the combination "would change the principle of operation of *Johnson's* system." Second Response at 53; ACP at 103-04. Patent Owner is again incorrect. As explained in the ACP, a person of ordinary skill in the art would have found motivation within *Johnson* to incorporate additional security mechanisms for communications over the Internet, such as interbusiness network communications. ACP at 103-04 (citing Request at 289-90). That person would have found in *Johnson* or *RFC 2401* identification of the same problem (improving security for Internet Protocol communications) as well as a solution to the same problem: an encryption and/or tunneling scheme. There is nothing in either reference that suggests that one must modify the essential features of the *Johnson* systems or change its principle of operation to implement IPSec in communications. Consequently, the Office's rejections of claims 9-11 and 13-16 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

6. Dependent Claim 21

The Office properly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered claim 21 obvious. In response, Patent Owner presents no response distinct from its response to claim 1. Because the rejection of claim 1 was proper, the Office's rejection of claim 21 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* also was proper and should be maintained. *See also* Request at 297-299.

7. Independent Claims 24, 26, 28 and 29

The Office correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render obvious claim 24. In response, Patent Owner presents no response distinct from to its responses to claims 1 and 2. Accordingly, because the Office's rejections of claims 1 and 2 were proper, its rejections of claims 24, 26, 28, and 29 were proper and should be maintained. *See also* Request at 301-304.

8. Dependent Claim 25 and 27

The Office correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render obvious claims 25 and 27. In response, Patent Owner presents no response distinct from to its responses to claims 1, 24, and 26. Accordingly, because the Office's rejections of claims 1, 24, and 26 were proper, the Office's rejections of claims 25 and 27 were proper and should be maintained.

III. There are No Secondary Considerations Linked to the Claims

The Office correctly found no nexus between the putative evidence of secondary considerations presented by Patent Owner and the claimed inventions. ACP 46-48. Its conclusions were correct, given that Patent Owner presented no evidence that any specifically claimed features of the claimed DNS systems could be identified as being attributable to any commercial success of any product or service.

The Office also was correct to not give any weight to the highly biased, self-interested and unsupported testimony of Patent Owner's Chief Technology Officer, Robert Short. Nothing identified by Patent Owner or its uncorroborated witness establishes with a legitimate evidentiary basis that any putative secondary considerations exist that can be attributed to any of the claimed inventions as distinguished from features of products and services known in the prior art, given that claims 1-29 encompass prior art DNS systems.

Finally, evidence of licensing or a jury verdict that is not the subject of a final judgment in concurrent litigation simply is irrelevant – neither constitutes "evidence of commercial success" much less evidence of secondary considerations relevant to the claims. MPEP § 716.03.

For all of the reasons set forth above, Patent Owner has not rebutted the Office's rejections of the claims on any of Issues 1-13, and that nothing raised in Patent Owner's Second Response merits reopening prosecution of the '181 patent. The rejection of all the claims under each of those Issues should, accordingly, be maintained.

Respectfully submitted,

/ Jeffrey P. Kushan /
Reg. No. 43,401
Attorney for Third Party Requester

SIDLEY AUSTIN LLP
1501 K Street, N.W
Washington, D.C. 20005
tel. (202) 736-8000/ fax (202) 736-8711
Date: April 23, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of	)	
U.S. Patent No. 8,051,181	)	Control No.: 95/001,949
Victor Larson et al.	)	Group Art Unit: 3992
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF SERVICE

I hereby certify that a copy of this correspondence for Comments by Third Party Requester Pursuant to Under 37 C.F.R. § 1.947 has been served in its entirety by First Class Mail on the following:

Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
901 New York Avenue, NW
Washington, DC 20001-4413

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile
April 23, 2013

Electronic Acknowledgement Receipt	
EFS ID:	15592827
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Rachel Heather Townsend/Jennifer Gordon
Filer Authorized By:	Rachel Heather Townsend
Attorney Docket Number:	41484-80200
Receipt Date:	23-APR-2013
Filing Date:	28-MAR-2012
Time Stamp:	16:31:56
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Third Party Requester Comments after Action Closing Prosecution	2013_04_23_Comments_3P_Requester_on_PO_Response.pdf	11826348 610caae766b3149f954c61fb06cc485d9962b9ac	no	50

Warnings:

Information:

2	Reexam Miscellaneous Incoming Letter	2013_04_23_Exhibit_A.pdf	9256623 cf57a5bd81fdaa147a93c5a4e99908fddc05f4d2	no	25
Warnings:					
Information:					
3	Reexam Certificate of Service	2013_04_23_Certificate_of_Service_flat.pdf	144101 ea113c4295e20e119feb6caa65510edcbf9d78a1	no	1
Warnings:					
Information:					
Total Files Size (in bytes):			21227072		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of
U.S. Patent No. 8,051,181
Larson et al.
Issued: November 1, 2011
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949
Group Art Unit: 3992
Examiner: Dennis G. Bonshock
Confirmation No.: 4522

COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. § 1.947

Mail Stop **Inter Partes Reexam**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On September 4, 2012, Patent Owner filed an overlength response ("First Response") to the June 4, 2012 Office action ("First Action"). On October 22, 2012, Requester filed a 45-page response with comments ("Comments") on Patent Owner's response. On January 16, 2013, the Office issued an Action Closing Prosecution ("ACP") that found claims 1-29 of U.S. Patent No. 8,051,181 ("the '181 patent") unpatentable. On March 18, 2013, the Patent Owner filed a second overlength response ("Second Response") and a petition under 37 C.F.R. § 1.183 seeking to waive the page limit rule for that response. Although the Office has not acted on the page-limit waiver as of the date of this submission, Requester provides these comments now to expedite conclusion of this proceeding. Requester believes no fee is due for this response, but authorizes the Director to debit any fee determined to be necessary from Deposit Account No. 18-1260.

I. General Comments on Errors that Pervade Patent Owner's Second Response

Throughout its Second Response, Patent Owner repeatedly makes several errors that should be given no weight in this proceeding.

First, Patent Owner asserts that several of the Office's positions in the ACP are new and require reopening of prosecution. This claim is baseless. As the Requester demonstrated in its March 27, 2013 Opposition to Patent Owner's Petition to Reopen Prosecution, each of the supposedly "new bases for [] rejections" issued by the Office are not new at all, but rather are identical to positions previously taken by the Office in its First Action or responses to unpersuasive criticisms by the Patent Owner. Indeed, the Second Response simply rehashes arguments Patent Owner and its expert presented earlier, advances unsupportable *legal* theories about the claims, or attempts, for the first time, to address issues that were ripe for response after the First Action. The Examiner should simply ignore these incorrect contentions. In this regard, Requester notes that Patent Owner submitted a Supplemental Declaration of Angelos D. Keromytis, Ph.D with its Second Response, but did not establish good and sufficient reasons why this affidavit is necessary or could not have been presented earlier. Under 37 CFR § 1.116(e), this affidavit should be barred. Indeed, the only basis Patent Owner presents for admitting this affidavit is that the Office has adopted new rejections, which, as explained herein and in Requester's March 27, 2013 Opposition, is demonstrably false.

It is the Requester's understanding that the Office will consider a petition to strike or exclude a Supplemental Declaration under 37 CFR § 1.116(e) to be premature if the Examiner has not yet issued an action determining whether to enter the declaration.[1] Rather than burdening the Office with such a petition now, Requester notes that Patent Owner has not shown good cause for submitting the declaration and that the Examiner should not admit or consider the new evidence or arguments presented in the Supplemental Declaration.

Second, as in its First Response, many of Patent Owner's arguments are premised upon alternative constructions of the claim elements, not adopted by the Office, that read limitations from the '181 specification into the claims. In particular, Patent Owner repeatedly argues that the Office should ignore Patent Owner's representations made during the prosecution of the '181 patent and during a reexamination of the '180 patent concerning the terms "secure name" and "unsecured name," and should instead construe those terms to include unclaimed limitations based on embodiments discussed in the specification. Not only did Patent Owner belatedly raise these claim construction arguments for the first time in the Second Response, Patent Owner's criticisms show that it fundamentally misunderstands the Office's policy of giving the claims their broadest reasonable construction. In proceedings before the Office, a patent owner must amend the claims to effectively exclude subject matter actually encompassed by the claim language. *See* MPEP § 2111 (explaining that under the broadest reasonable construction practice used in PTO proceedings, ". . . applicant has the opportunity to amend the claims during

[1] *See* Decision on Petitions in 95/001,788 at 8 (Mar. 26, 2013).

prosecution, [and that] giving a claim its broadest reasonable interpretation will reduce the possibility that the claim, once issued, will be interpreted more broadly than is justified.") (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984).

Patent Owner's arguments in this case vividly demonstrate why this rule is followed – all of Patent Owner's arguments before the Office seek to impermissibly import unclaimed limitations, requirements, meanings, disparagements or disclaimers into the claims in order to narrow their scope and avoid the prior art, now that the claims have been found – based on their actual language – to encompass what is disclosed in or rendered obvious from the prior art. *See* M.P.E.P. § 2111.01(II); *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969). If Patent Owner is unsatisfied with the meaning of the claims as they are written, Patent Owner should seek to amend the claims to correspond to the meaning(s) Patent Owner desires them now to have instead of asking the Office to simply ignore its well-established practices in construing a claim's scope. Allowing the Patent Owner to recast its claims without actually amending them would violate the Office's well-established practice of requiring a patentee to expressly incorporate limitations in the claim language to effectively limit their scope in these proceedings, and would prevent the Office and Requester from evaluating the newly claimed subject matter for compliance with 35 U.S.C. § 112. Consequently, Patent Owner's requests that the Office depart from its well-established practices must be uniformly rejected.

II. The Rejections of the Claims Were Proper

A. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-12, 14, 15, and 17-29 Based on *Beser* (Issue 1).

1. Independent Claim 1

In the ACP, the Office correctly maintained its determination that *Beser* anticipates claim 1. In response, Patent Owner asserts *Beser* does not teach a system that discloses (1) "a first device," "a second device," "a message from [the] second device of the desire[] to securely communicate with the first device" or "sending a message over a secure communication link from the first device to the second device." Second Response at 2-6. Each of these assertions is incorrect.

a. *Beser* Discloses "a First Device," "a Second Device," and "a Message from [the] Second Device of the Desire[] to Securely Communicate With the First Device"

The Office correctly found that *Beser* discloses both "a first device" and "a second device." ACP at 17-19. For example, *Beser* illustrates its system in Figure 1, which shows two edge routers (14 and 16), each linked to a different communication device (24 and 26, respectively). These devices are used to communicate with each other over a secure network established, *inter alia*, using the trusted third party networking device (30). *Beser* at Fig. 1. Either the communication devices (items 24 and 26) or the edge routers (items 14 and 16) can qualify as a "first" and "second" devices, respectively, under the plain meaning of the claims, which impose <u>no restrictions</u> on the properties or capabilities of the "first" or "second" devices.

The Office also correctly found that *Beser* shows a method where a "message from a second device of *the desire* to securely communicate with the first device" is "received, at a network address corresponding to the secure name associated with the first device." ACP at 18. For example, the Office correctly found that *Beser* shows an originating device (items 24 or 14) (a "second device") that sends a message requesting a connection with a destination device (items 16 or 26) (a "first device") to a trusted third network device. *Beser* at 11:25-32. The trusted third party network device routes the request to the destination edge router (16) associated with the destination communication device (26) (a "network address corresponding to the secure name associated with the first device"). *Id.* If the connection is authorized, the trusted third party network device facilitates establishment of a secure communication link between the originating and destination communication devices. *Id.* Finally, the Office correctly found that *Beser* discloses that, after the secure link is established, *a different message* (*e.g.*, packets containing data representing a VOIP communication) is sent from the originating device to the destination device using the secure communication link ("sending a message over a secure communication link from the first device to the second device").

Patent Owner has not disputed any of these findings. Instead, Patent Owner asserts the Office and the Requester have improperly read the claim language, mischaracterized its arguments or misapplied the law of anticipation. These assertions are spurious.

First, Patent Owner italicizes several passages in claim 1 (*e.g.*, a "first device," the "desire to securely communicate" "from the second device") and asserts these are not shown in *Beser*. Second Response at 2. These contentions border on the incomprehensible. For example, Patent Owner may be contending that because *Beser* does not label its originating device as a "second" device or does not label its destination device as a "first device," *Beser* cannot anticipate the claims. This semantic distinction is meaningless, and must be rejected. Under the plain meaning of claim 1, the originating device shown in *Beser* (the device that sends the message) qualifies as a "second" device within the meaning of the claims because it sends a message requesting a connection to a destination device, which qualifies as a "first device" within the meaning of the claims.

Next, Patent Owner contends the Office erred by finding that the claims merely require a message to be sent between the two devices. Here, Patent Owner mischaracterizes the Office's findings and ignores what is actually shown in *Beser*. Specifically, *Beser* shows a first message containing a request to communicate with a destination device is sent by the originating device. *Beser* at Fig. 6. This meets the claim requirement of a "message of the desire to securely communicate" with the destination device. Then, *Beser* shows that a different message is sent from the trusted third party device to the edge router providing access to the destination communication device which starts the process of negotiation of the secure connection. *Id.* *Beser* also shows a different message (*e.g.*, the data representing the content of the VOIP communication) is sent by the originating device to the destination device *after* the secure connection is established. *Id.*; *id.* at 4:44-54. Thus, even under Patent Owner's reading of the claims, *Beser* plainly anticipates this feature of claim 1. Of course, there is nothing in claim 1 that excludes the messages being sent in the *Beser* systems. Moreover, based on the claim language, the first message may have the same content as a subsequent message.

Patent Owner also contends the Request and the Office improperly conclude that multiple devices may qualify as "first" or "second" devices. This again is a spurious complaint. Nothing in the claims precludes a "device" from being an edge router, a communication device or both working in conjunction. In fact, the '181 patent itself illustrates the claimed systems by showing devices on a local network communicating with remote destination using edge routers – precisely what is shown in *Beser*. Compare *Beser* at Fig. 1 to '181 Patent at 51:15-29 and Fig. 28. Patent Owner also disputes the Office's conclusion that the various devices shown in *Beser* may "at any particular point" qualify as a first or second device. In reality, there is nothing in the claims that precludes reading the claims as encompassing these various embodiments described in *Beser*. For example, nothing in the claim precludes intermediary devices on a network path from being a first or second "device." And Patent Owner's complaint that the Office and the Request "never identified the alleged first device and the alleged second device in *Beecher*" is simply false. Second Response at 3. All of these documents point out precisely how features of the *Beser* precisely match the requirements of the claims. For example, as explained in the Request, First Action, and ACP, *Beser* discloses both a "first device" and a "second device" that meet the limitations of the claims. Request at 27-29; First OA at 6-7, ACP at 18-19 (citing *Beser* at 11:26-12:19). In the *Beser* systems, when an "originating telephony device" makes a request to securely communicate with a "terminating telephony device," the request is brokered by intermediary devices, including a "first network device," a "second network device," and a "trusted-third-party device." *Beser* at Fig. 6. The request is a message containing the "unique identifier" for the "terminating telephony device." *Beser* at 11:25-32. When the "trusted-third-party device" receives the message, it uses the "unique identifier" to look up a public IP address for a "second network device" that is associated with the "terminating telephony device," and then it sends the message requesting a secure connection to the "second network device." *Beser* at 11:26-32 ("A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at step 116. The second network device 16 is associated with the terminating telephony device 26."). The "second network device" receives the message requesting a secure connection and then negotiates the tunneling association for the "terminating telephony device." *Beser* at Fig. 6; 11:59-62. The result of the creation of the tunneling associating is that the "terminating telephony device" and the "originating telephony device" (the "first" and "second" devices) can send and receive messages over the secure connection. Thus, contrary to Patent Owner's assertions, the Office and Requester have not been "picking and choosing among different devices in *Beser*." Instead, they have been comparing <u>what is actually claimed</u> to <u>what is actually disclosed</u> in *Beser*.

Patent Owner's next contention is similarly flawed. Specifically, Patent Owner disputes the observation made in the Request and by the Office that there is no restriction in the claims precluding either the edge router or the communication device, or both working together, from being a first or a second device within the meaning of the claims. Second Response at 4. Patent Owner misunderstands this point, reading it as suggesting that a single device in the *Beser* system (*e.g.*, one edge router or one communication device) can be both a first and second device. The point made by the Office (and Request) is that either the communication device or the edge router or both working together can be <u>one device</u> within the meaning of the claims. That one device then will communicate securely with a <u>different</u> edge router/communication device/combination (the "second" device). Patent Owner's criticisms here can be disregarded.

Much of Patent Owner's argument rests on its belief that it is appropriate for the Office to read unclaimed limitations into the claims to distinguish them from the prior art. The Office has correctly rejected this theory. If Patent Owner wishes to exclude the subject matter described in *Beser* from the scope of its claims, it must amend those claims to contain language that expressly does so. As the claims presently read, they do not, and the rejections for anticipation by *Beser* are thus proper and should be maintained. Consequently, the Office correctly found that *Beser* discloses "a message from [an originating telephony device] of the desire to securely communicate" is received "at [the] network address corresponding to the [unique identifier] associated with [the terminating telephony device]." Similarly, the Office correctly found that *Beser* shows "sending a message over a secure communications link from the [terminating telephony device] to the [originating telephony device]." Accordingly, *Beser* describes a system that provides "a first device," "a second device," and "a message" as required by the claims.

b. *Beser* Discloses "Sending a Message Over a Secure Communication Link from the First Device to the Second Device."

The Office correctly maintained its determination that *Beser* discloses "sending a message over a secure communication link." In response, Patent Owner presents the same arguments it presented in response to the First Action; namely, that *Beser* does not describe a "secure communication link" because (1) "the broadest reasonable interpretation of secure communication link requires encryption, and *Beser's* tunneling association is not encrypted" and (2) "even if the Office maintains that a secure communication link does not require encryption, *Beser*'s tunneling association still is not a secure communication link." Second Response at 5. For reasons the Office has already conveyed, both of these contentions are incorrect.

Patent Owner first repeats its flawed reading of *Beser*; namely, that it "teaches away from using encryption in its tunneling system." *Id.* As the Office correctly determined, the passages cited by Patent Owner do not "teach away" from the use of encryption in IP tunneling associations. Rather, what those passages explain is that only in <u>certain high data volume</u> situations can the use of encryption demand additional computational capacity to implement. As was explained in Requester's comments and the ACP, the claims are not limited to high data volume applications, but encompass communications of any magnitude. ACP at 20. The cautionary observations in *Beser* about <u>certain</u> types of data communication applications are thus irrelevant to what is <u>actually claimed</u>.

Moreover, Patent Owner again mischaracterizes the teachings in *Beser* about use of encryption in IP tunneling. As the Office explained, *Beser* consistently and repeatedly points out that use of legacy encryption techniques in IP tunneling schemes is conventional and ordinarily should be used. The Office found that *Beser* "specifically teaches utilization of encryption in combination with the tunneling, where this tunneling is being used as an additional means of making the channel for transmission secure . . . ." ACP at 20 (emphasis added). Although *Beser* does indicate that there may be practical challenges using encryption in some circumstances, this concern is not an express teaching to never use IPSec or other encryption-based IP tunneling models, or that the *Beser* techniques are only an alternative to using encryption—a conclusion with which the Patent Office has consistently agreed. ACP at 21; *see also* Action Closing Prosecution of 95/001,788 ("'788 ACP") at 32.[2] Instead, *Beser*'s tunneling scheme is to be "used in combination with legacy encryption to ensure data security." ACP at 20.

Patent Owner also contends that "even if a secure communication link [does] not require encryption" then "*Beser's* tunneling scheme still does not disclose a secure communication link." Second Response at 6. Yet, as explained in the Request, the inventive tunneling method shown in *Beser* "is designed to protect the integrity of the private IP address and ensure the anonymity of the terminating devices." Request at 26. Moreover, the Office correctly found that *Beser*'s systems "provide[] an additional layer of security by not only encrypting data but hiding the source and destination IP addresses." ACP at 21. Accordingly, *Beser* discloses "a secure communication link." Patent Owner offers no new arguments, but merely repeats the same baseless assertions it made in its First Response about *Beser* not providing secure communication links. Those assertions are not only refuted by the express teachings in *Beser*, they rest on unclaimed limitations and features of the claims. The Office properly rejected Patent Owner's assertions when they were made in the previous Patent Owner response, and should do so again. Thus, because the Office properly found that *Beser* discloses all the limitations of claim 1, its finding of anticipation of claim 1 was proper and should be maintained.

2. Independent Claim 2

The Office correctly found that *Beser* discloses every limitation of independent claim 2. Patent Owner does not present any new or distinct response to the rejection of claim 2, but

[2] U.S. Patent No. 7,418,504 to Larson, which is at issue in the '788 reexamination, is derived from the same applications as U.S. Patent No. 8,051,181 to Larson.

instead refers to its arguments regarding claim 1. Because claim 1 was properly rejected, the Office's finding of anticipation of claim 2 was proper and should be maintained.

3. Dependent Claim 4

The Office correctly found that *Beser* discloses every limitation of dependent claim 4. Patent Owner disagrees, arguing that *Beser*'s "unique identifier" does not "indicate anything about security." Second Response at 7. Patent Owner's argument is an immaterial variation of the argument it made in its First Response that *Beser* does not disclose a "secure name service" which the Office properly rejected. *See* First Response at 12-13; ACP at 21-22.

Patent Owner's assertions also are refuted by the teachings of *Beser*. As explained in the Request, the first network device and the trust-third-party device can recognize the "unique identifier" as being secure and can then implement protocols to obfuscate it from discovery by untrusted parties:

> "For each transfer of a packet from the first network device 14 to the trusted-third-party network device 30, the first network device 14 constructs and IP 58 packet. . . . <u>The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12</u>." Request at 36 (quoting *Beser* at 11:13-25).

Thus, because *Beser* recognize that security must be implemented for certain "unique identifiers," *Beser* discloses that "the secure name indicates security."

In addition, *Beser*'s "unique identifier" is clearly within the scope of Patent Owner's construction of the term "secure name." As the Office observed in the <u>First Action</u>, Patent Owner asserted during prosecution of the related '180 patent that the term "secure name" could be construed to include "*a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number.*" First Action at 5. Requester has explained that *Beser*'s "unique identifier" could be a non-standard domain name such as a secure domain name or it could be an E.164 phone number, and the Office has adopted this conclusion. Order at 5-6; Request at 35-36. As described above, the *Beser* systems can recognize that security must be implemented for certain "unique identifiers"—which would include secure domain names or phone numbers. Thus, *Beser* discloses that "the secure name indicates security." Consequently, the Office's rejection of claim 4 as anticipated by *Beser* was proper and should be maintained.

4. Dependent Claim 5

The Office correctly found that *Beser* anticipates every limitation of dependent claim 5. In response, Patent Owner admits that *Beser* discloses encrypting messages sent to the trusted-third-party device, but argues that, for the "the message containing the network address associated with the secure name of the second device," *Beser* does not disclose "receiving the message in encrypted form." Second Response at 7-8. Patent Owner's argument is again an immaterial variation of its unpersuasive assertions on this point in its First Response, which the Office properly disregarded. Again, Patent Owner's argument is based on an incorrect reading of *Beser*. As the Office explained, *Beser* discloses encrypting "IP packets 58 [*sic*]," which would include any of the packets sent in establishing the secure communications link that contained the "unique identifier," "public IP 58 addresses," or "private IP 58 addresses." ACP at 23. In response to such a query, the third-party-trusted device would return a message containing the "public IP 58 address" associated with the "unique identifier" of the query. Thus, *Beser* discloses that the message received by the first network device can be encrypted. Accordingly, *Beser* discloses that "the message containing the network address associated with the secure name of the second device" is "receiv[ed] . . . in encrypted form." Consequently, the Office's rejection of this claim was proper and should be maintained.

5. Independent Claims 24, 26, and 29

In response to the rejection of claims 24, 26, and 29, Patent Owner presents no distinct responses from those offered in claim 1. Because the rejection of claim 1 was proper, the rejections of claims 24, 26, and 29 based on *Beser* also were proper and should be maintained.

6. Independent Claim 28

In response to the rejection of claim 28, Patent Owner presents no distinct response from those offered in claim 2. Because the rejection of claim 2 was proper, the rejection of claim 28 based on *Beser* was also proper and should also be maintained.

7. Dependent Claims 3, 6-12, 14-15, 17-23, 25 and 27

Patent Owner presents no distinct response to the rejection of claims 2-3, 8, 12, 14-15, 17 and 19-22 based on *Beser* relative to its response to the rejection of claim 2. Consequently, because the rejections of those claims were proper, the Office's rejections of claims 3-4, 8, 12, 14-15, 17 and 19-22 based on *Beser* were proper and should be maintained. Request at 35-45.

B. Response to Patent Owner's Arguments Regarding Rejection of Claims 1, 2, 6-9, 12-17, and 24-29 Based on *Mattaway* (Issue 3).

1. Independent Claim 1

Mattaway describes methods and systems for establishing a secure communication link between two devices across a public network such as the Internet. *See* Request at 68-72; ACP at 30-34. The Office correctly maintained its determination that *Mattaway* describes a system that anticipates claim 1. In its Second Response, Patent Owner asserts again that *Mattaway* does not teach a system that discloses (1) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, (2) "[a] first device associated with a secure name and an unsecured name" Second Response at 9-12. Both assertions are incorrect.

a. *Mattaway* Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"

Patent Owner's first response is that the Office has changed its position on what *Mattaway* teaches. Specifically, Patent Owner asserts that in the First Action, the Office cited the <CONNECT REQ> message in *Mattaway* as disclosing the "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device." Second Response at 9. Patent Owner contends the Office has now taken a new position in explaining that the desire to securely communicate is received at the first device in the form of the <CALL> message. Patent Owner is wrong. The explanation provided by the Office in the ACP was plainly in response to Patent Owner's disingenuous criticism of what *Mattaway* teaches. For example, Patent Owner argued that in *Mattaway* there was no disclosure that the desire to securely communicate represented by the <CONNECT REQ> message was ever "received at a network address corresponding to the secure name associated with the alleged first device." Response at 21. In response, the Requester (and Office) pointed out that the <CONNECT REQ> message, *i.e.*, the "desire[] to securely communicate," is received at the first device in the form of the <CALL> message. This is confirmed by Figure 17A (which Patent Owner wrongly states stands for the opposite proposition), as <CALL> is shown as the step (Step 8) following the

<CONNECT REQ> and <CONNECT ACK> (Steps 6 and 7A) messages identified in the Request. This is also confirmed by the *Mattaway* specification. *Mattaway* at 23:42-24:42.

Moreover, the Request explained that after receiving the IP address of the first device, the second device may "directly establish the point-to-point Internet communications with the [first device] using the IP address of the [first device]." Request at 72; ACP at 33-34. *Mattaway* discloses these "point-to-point Internet communications" are accomplished by the second device "open[ing] up a socket" to the first device. *See Mattaway* at col.24, ll.15-30; ACP at 33-34. The second device transmits a "<CALL>" packet to the first device, to which the first device may, among other things, acknowledge or reject the call. *Mattaway* at col.24, l.11 – col.25, l.12; ACP at 33-34. Patent Owner simply ignores this observation in its response.

Patent Owner also asserts that neither the <CONNECT REQ> message nor the subsequent <CALL> message "include any information related to security." Second Response at 10; *see also id.* at 11. The Office properly rejected that theory because nothing in the claim language requires that the messages themselves have "information related to security." The process disclosed in *Mattaway* "enables the parties to converse in real-time, telephone quality, encrypted communication over the Internet and other TCP/IP based networks." *Mattaway* at col.25, ll.32-34; Request at 72; ACP at 34. Therefore, *Mattaway* discloses a message from the "second device" of the "desire to securely communicate" pursuant to claim 1. This reading of *Mattaway* is also consistent with Patent Owner's approach in concurrent litigation, where it has asserted that because Apple's "FaceTime calls are encrypted for secure communication . . . any request to make a FaceTime call is a request expressing the desire to securely communication using FaceTime." Exhibit A[3] at 2. Patent Owner cannot have it both ways, and its assertion that the message itself must "include . . . information related to security" must be given no weight in view of its contrary assertions on infringement against Requester.

b. *Mattaway* Discloses "A First Device Associated With A Secure Name and An Unsecured Name"

Patent Owner next asserts that *Mattaway* "does not disclose a secure name," because "those [are] names [that] are used to communicate securely that are resolved by a secure name

[3] Exhibit A constitutes Patent Owner's Evidence of Infringement against Requester filed with its Complaint in ITC investigation 337-TA-858, In re *Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing Same.*

service," and that "the connection server 26 of *Mattaway* . . . is a conventional server of the type distinguished by the '181 patent specification." Second Response at 11. These assertions can simply be ignored because they are predicated on Patent Owner's belief that the claims incorporate specific requirements regarding the claimed "secure name" which are not actually recited in the claims. As to the first point, the Office properly found that Patent Owner's representations regarding "secure name" here are inconsistent with those it made during prosecution when it told the Patent Office a "secure name" could be "as simple as a telephone number." ACP at 32. Patent Owner's contentions here also are entirely inconsistent with its assertions in concurrent litigation. Specifically, Requester asserted in an action it commenced in the ITC against Requester that:

> The <u>secure name</u> of the device is related to the <u>caller's email address</u> or, for Accused iPhones, the <u>caller's telephone number</u>. The Apple servers which facilitate the FaceTime function store a plurality of secure names and associated network addresses. A prospective caller's registration for FaceTime use using an email address or telephone number constitutes a request for registration of a secure name for the Accused Device used by the caller.

Exhibit A at 10 (emphasis added). As to the latter point—that *Mattaway's* servers are "conventional"—Patent Owner asks the Office to treat its "disclaimer" of conventional servers as an effective claim limitation that excludes subject matter which the language in the claims actually encompasses. *See* Second Response at 11-12. Because it has not proposed to amend its claims, these efforts to read limitations into them to exclude the embodiment of the "secure name" shown in *Mattaway* must be rejected.

Patent Owner also contends (again) that the secure name disclosed in *Mattaway* (an e-mail address) "is not associated with the first device." Second Response at 12. The Office correctly rejected this assertion in the ACP, explaining that "email addresses" are utilized in *Mattaway* to obtain IP addresses from the connection server, ACP at 31, and that a "user may use an alias to access the secured data under the firewall, where the secured data includes email addresses and IP addresse[s]." ACP at 32. The devices shown in *Mattaway* (webphones) are each required to register information as part of the <USER INFO REQ> message. *Mattaway* 22:65-23:5, 40:27. *Mattaway* thus discloses that information requested from the first device/Webphone client would include an encrypted email address. Accordingly, *Mattaway* discloses "a first device associated with a secure name and an unsecured name." The Office's rejection of claim 1 based on *Mattaway* thus, was proper and should be maintained.

2. Independent Claim 2

In the ACP, the Office correctly found that *Mattaway* discloses every limitation of dependent claim 2. In response, Patent Owner presents no distinct response to the rejection of claim 2 based on *Mattaway* relative to its response to the rejection of claim 1. Because the Office's rejection of claim 1 over *Mattaway* was proper, its rejection of claim 2 over *Mattaway* also should be maintained.

3. Independent Claims 24, 26, 28, and 29

In the ACP, the Office correctly found that *Mattaway* discloses every limitation of independent claims 24, 26, 28 and 29. In response, Patent Owner presents no distinct response relative to its response to the rejection of claim 1 over *Mattaway*. Because the rejection of claim 1 over *Mattaway* was proper, the Office's rejection of claims 24, 26, 28, and 29 over *Mattaway* also was proper and should be maintained.

4. Dependent Claims 7-9, 12-17, 25, and 27

In the ACP, the Office correctly found that *Mattaway* discloses every limitation of dependent claims 7-9, 12-17, 25, and 27. In response, Patent Owner presents no distinct response relative to its response to the rejection of claims 2, 24, and 26 over *Mattaway*. Because the Office's rejection of claims 2, 24, and 26 over *Mattaway* was proper, its rejection of claims 7-9, 12-17, 25, and 27 over *Mattaway* also was proper and should be maintained.

C. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3-4, 10-11, 18 and 23 Based on *Mattaway* in view of *Beser* (Issue 4).

1. Dependent Claim 4

In the First Office Action, the Office correctly found that *Mattaway* in view of *Beser* describes a system that would render claim 4 obvious to a person of ordinary skill in the art. In its First Response, Patent Owner asserted only that "*Beser* does not make up for the deficiencies noted above regarding *Mattaway's* disclosure." Response at 28-29. Understandably, the Office did not find this argument persuasive. Now, it its Second Response, Patent Owner contests for the first time the substantive findings set forth in the First Action regarding *Mattaway* in view of *Beser*, contrary to the requirements of 37 C.F.R. 1.951. *See* 37 C.F.R. 1.951 ("the patent owner may once file comments limited to the issues raised in the Office action closing prosecution.") Patent Owner's belated response should be disregarded.

Even if Patent Owner's belated response is considered, it should be rejected as unpersuasive. First, Patent Owner contends that *Beser* does not show that the unique identifier used in its schemes "indicates security." Second Response at 13. Yet, *Beser* plainly teaches that its scheme – in which the unique identifier plays a critical role – provides security, *inter alia*, through obsfucation of internal IP addresses of the originating and destination communication devices. *See* Request at 96. A person of ordinary skill in the art would have plainly recognized from that description that the unique identifier is associated with secure communications. Moreover, the Office did not rely on "conclusory" statements to support the rejection of claim 4. Second Response at 13. Instead, as explained in the Request, *Mattaway* recognizes the importance of using encrypted communications in its system to secure the data that is exchanged. Request at 96. *Beser* also recognized the importance of securing the data being transmitted in its system, and explained that a further measure of security could be achieved through obfuscation of the unique identifier, *i.e.*, the "secure name" of *Beser*. Request at 96. Thus, the Request explained in detail why a person of ordinary skill would have considered it obvious to use the obfuscation techniques described in *Beser* in which the unique identifier "indicates security" in the *Mattaway's* scheme, which, like *Beser,* emphasizes security. Thus, the Office's rejection of claim 4 was proper and should be maintained.

2. Dependent Claim 10

In the ACP, the Office correctly maintained its determination that *Mattaway* in view of *Beser* would have rendered claim 10 obvious to a person of ordinary skill in the art. Claim 10 recites "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." As explained in the Request, a person of ordinary skill in the art would have found motivation within *Mattaway* to modify the encrypted communications disclosed therein to incorporate additional mechanisms of protection in order to provide a more secure communication link. Request at 96-97; ACP at 51-53. That person would have found that *Beser* identified the same problem (improving security of network communications) and provided a solution to that problem; namely, to use a particular type of IP tunneling.

Again, rather than contesting any of these points in its First Response, Patent Owner now belatedly challenges these substantive findings that were set forth in the First Office Action. The Office should disregard these comments pursuant to Rule 951. Even if those comments are considered, they should be disregarded as being unpersuasive. Indeed, Patent Owner's only argument is premised on the assumption that the secure communication link disclosed in *Mattaway* could not include the communication link between the server that facilitates the secure communication link. Nothing in the description of *Mattaway* would preclude that embodiment. Accordingly, the Office's rejection of claim 10 was proper and should be maintained.

3. Dependent Claims 3, 11, 18, and 23

In the ACP, the Office correctly found that *Mattaway* in view of *Beser* discloses every limitation of dependent claims 3, 11, 18 and 23. In response, Patent Owner presents no distinct response relative to its response to the rejection of claim 2 over *Mattaway* in view of *Beser*. Accordingly, because the Office's rejection of claim 2 was proper, its rejection of claims 3, 11, 18 and 23 based on *Mattaway* in view of *Beser* also was proper and should be maintained.

D. Response to Patent Owner's Arguments Regarding Rejection of Claims 10 and 11 Based on *Mattaway* in View of RFC 2401 (Issue 5)

1. Dependent Claim 10

In the ACP, the Office correctly maintained its determination that *Mattaway* in view of RFC 2401 would have rendered claim 10 obvious to a person of ordinary skill in the art. Claim 10 recites "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." As explained in the Request, a person of ordinary skill in the art would have found motivation within *Mattaway* to modify the encrypted communications disclosed therein to incorporate additional mechanisms of protection in order to provide a more secure communication link. Request at 98-99; ACP at 54-55. That person also would have recognized that RFC 2401 addresses the same problem – improving security of networked communications – and provides a solution to that problem; namely, use of a particular type of tunneling.

Again, Patent Owner's belated comments should be disregarded as they were not presented in response to this ground of rejection when it was imposed in the First Office Action. They also should be rejected as being incorrect. Indeed, Patent Owner assertions are premised on the mistaken belief that the secure communication link disclosed in *Mattaway* could not include a communication link with the server that facilitates the secure communication link.

Nothing in the description of *Mattaway* precludes such a configuration. Accordingly, the Office's rejection of claim 10 was proper and should be maintained.

2. Dependent Claim 11

In the ACP, the Office correctly found that *Mattaway* in view of RFC 2401 discloses every limitation of dependent claim 11. In response, Patent Owner presents no distinct response relative to its response to the rejection of claim 2 based on *Mattaway* in view of RFC 2401. Accordingly, because its rejection of claim 2 was proper, the Office's rejection of claim 11 based on *Mattaway* in view of RFC 2401 also was proper and should be maintained.

E. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-9, 12-15, and 18-29 Based on *Lendenmann* (Issue 6).

1. Independent Claim 1

The Office correctly maintained its determination that *Lendenmann* describes a system that anticipates claim 1. In response, Patent Owner repeats and expands upon arguments it made in its First Response, namely that (1) *Lendenmann* does not teach a system that discloses "[a] first device associated with a secure name and an unsecured name" and (2) the Office has relied on "multiple unrelated features as corresponding to the 'first device' recited in claim 1." Second Response at 15-20. These arguments are not materially different from the arguments the Office previously found unpersuasive. They also rest on incorrect characterizations of *Lendenmann* and are inconsistent with Patent Owner's own representations before the Patent Office.

a. *Lendenmann* Discloses "A First Device Associated With A Secure Name and An Unsecured Name"

Patent Owner advances three different arguments as to why *Lendenmann* does not disclose a first device associated with a secure name and an unsecured name. Second Response at 16-18. Each argument should be disregarded.

<u>First</u>, Patent Owner contends the Office has misconstrued the terms a "secure name" and an "unsecured name. " The Office properly rejected this argument when Patent Owner made it in its First Response, and should do so again. Patent Owner's new theories about what its claims mean or do not mean, and how those claims relate to *Lendenmann* should be disregarded, not only because they are untimely pursuant to 37 C.F.R. 1.951, but because they ignore what the claims actually specify.

In its Second Response, Patent Owner strenuously disputes the Office's conclusions about the broadest reasonable construction of the terms "secure name" and "unnsecure name." The reason is simple – under the meanings employed by the Office, the claims encompass the systems described in *Lendenmann*, and are anticipated by this prior art.

For example, Patent Owner contends it was improper for the Office to use the Patent Owner's own representations about what the claim terms "secure name" and "nonsecure name" mean. Patent Owner is simply wrong – its own statements about these terms are highly probative evidence about what the terms do or do not reasonably encompass under their broadest reasonable construction.

As explained in the First Action and ACP, Patent Owner represented to the Office that a "secure name" may be any type of non-standard name. Under that interpretation, a "secure name" may be an X.500 name. ACP at 56; Request at 22; Order at 5 (Patent Owner asserted terms are not indefinite because a "secure name" could be "a secure non-standard domain name" or a "telephone number."). In response, Patent Owner asks the Office to disregard its previous representations that were made to secure allowance of these claims and analogous statements made during reexamination in the '180 patent, and instead import restrictions into the claims from particular examples in its specification. For example, Patent Owner contends that its prior statement that a "secure name" could be "a secure non-standard domain name" or a "telephone number" should be ignored because that statement "merely illustrate[s] exemplary differences between a 'secure name' and a 'secure domain name' in response to an indefiniteness rejection." Second Response at 16.

Patent Owner's statements were not limited as it contends. Rather, Patent Owner asserted that the term was not indefinite because one would recognize it could encompass "a secure non-standard domain name" or a "telephone number." The Office correctly found that because a X.500 name is a "non-standard domain name," it is a "secure name" within the meaning of the claims. Similarly, when Patent Owner's claims in a related patent (the '180 patent) were being rejected over the prior art, Patent Owner made unconditional statements about what the specification of the '180 patent (which is the same as the specification of the '181 patent) said a "secure" and "unsecure" name could be. As Patent Owner stated:

> The '180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a convention[al] domain name server using a secure domain name will result in a

> return message indicating that the URL is unknown ('180 patent at 51 :25-35) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name ('180 patent at 51:25-35).

Request at 22. These comments are probative here not only because Patent Owner advanced the same construction in the '180 reexamination proceeding that it advanced during prosecution of the '181 patent, but because these comments reflect Patent Owner's characterization of what the common specification of the '180 and '181 patents says these terms mean.

Patent Owner asks the Office to disregard those past statements, and instead read material limitations into the claims from specific examples shown in the specification. Patent Owner attempts to justify this request by asserting the construction used by the Office and Requester "removes all meaning of 'secure' and 'unsecure' from the claim terms." Second Response at 16. Patent Owner is incorrect. The meanings for these terms that Patent Owner advanced previously to the Office are not incompatible with the claim language. For example, claim 1 uses the term "secure name" to identify the destination of a message. *See* claim 1 ("receiving, at a network address corresponding to the secure name associated with a first device, a message from a second device"). Similarly, in claim 2, the term is used to identify a device. *See* claim 2 ("from the first device, sending a message to a secure name service, the message requesting a network address associated with a secure name of the second device..."). The use of "unsecure" or "secure" names to serve these identification functions is not incompatible with the claim language. In fact, Patent Owner actually uses the precise meaning it advanced during the prior proceedings in a dependent claim. Specifically, claim 23, which depends from claim 2, specifies that a "the secure name of the second device is a secure, non-standard domain name.") Thus, Patent Owner's assertions that the meanings used by the Office and in the Request for "unsecure" and "secure" names are somehow incompatible with its disclosure are simply false.

Patent Owner's examples of contradictions between its specification and the claim language can be easily rejected. For example, Patent Owner asserts that in one example shown in the '181 specification, a top-level domain name is replaced with a secure domain name in order to establish a secure communication link, and then after that communication link is terminated, the secure domain name is replaced with a non-secure domain name. Second Response at 16-17. This example has no relevance to what Patent Owner has actually claimed because there is no claim limited to this precise sequence of steps Patent Owner describes.

Patent Owner's arguments thus can be easily dismissed – they do not compare what is actually claimed to the prior art, but instead compare unclaimed features in the specification to the disclosure in *Lendenmann*. In fact, the example from the '181 specification cited by the Patent Owner here illustrates use of a non-standard domain name as a secure name to establish a secure connection. Moreover, under the broadest reasonable construction used by the Office, the claims do not necessarily exclude this "replacing" embodiment. *See* M.P.E.P. § 2111.01(II); *Superguide Corp. v. DirecTV Enterprises, Inc.*, 358 F.3d 870, 875, 69 USPQ2d 1865, 1868 (Fed. Cir. 2004) ("Though understanding the claim language may be aided by explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim. For example, a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment."). Nor is anything in Patent Owner's example inconsistent with the Office's determination that a "secure name" may be a non-standard domain name or a phone number. Simply put, if Patent Owner believes the claims as written are overly broad, it must amend those claims instead of attempting read unclaimed limitations from the specification into them.

Second, the Patent Owner argues *Lendenmann* does not disclose a device that has both a "secure name" and an "unsecure name." Specifically, while Patent Owner acknowledges that *Lendenmann* refers to both X.500 and DNS as naming schemes, it asserts there is no "nexus between X.500 names and secure communications" shown in *Lendenmann*. Second Response at 17. The Office has already rejected this argument, finding that "X.500 satisfies the requirement for a secure name, as the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address." ACP at 58. The Office also explained that the X.500 naming scheme of the DCE environment "is a secure, internal naming convention." ACP at 58 (citing Request at 105). For example, the Request explained that resolution of the X.500 names is controlled by the CDS, which is integrated into the security server of the X.500 system and will only complete an operation "if the user is authenticated and authorized." Request at 104. Thus, as explained in the ACP and the Request, DCE cells, as well as the objects within them, can have both an X.500 name (a "secure" name) and a DNS name (an "unsecure" name), and the Office correctly found that *Lendenmann* discloses "a first device associated with a secure name and an unsecured name."

Third, Patent Owner argues that *Lendenmman* does not disclose "secure" names because it does not "hid[e] Internet addresses" and does not disclose accessing Internet addresses outside of the DCE environment. Patent Owner's arguments can be dismissed based on the Office's construction of the term "secure name" and the actual teachings of *Lendenmann*.

A name may be found to be secure if it is stored in a secure location and whether it can be resolved by a conventional name server. X.500 names satisfy this definition. As *Lendenmann* explains, addresses in its system are hidden because queries to the CDS, which is integrated into the security server, are made within the confines of the DCE cell and can also be encrypted. ACP at 58-59. Further, whether the *Lendenmann* systems access Internet addresses outside of the DCE environment has no relevance to the question whether *Lendenmann* discloses a device having a "secure name" and an "unsecure name." *Lendenmann* presents the X.500 scheme, which is "a secure, internal naming convention," and the DNS scheme, which is a naming convention based on the public Internet DNS system is unsecure (*e.g.*, because conventional name servers are publicly accessible and resolve conventional domain names in a manner that provides no inherent security). Because Patent Owner's arguments are all based on improper claim constructions and a misunderstanding of the *Lendenmann* systems, the Office should disregard them and maintain the rejection of claim 1 as anticipated by *Lendenmann*.

b. *Lendenmann* Discloses "a First Device" as required by Claim 1

For the first time, Patent Owner asserts that *Lendenmann* does not disclose a "first device," contending that Office has improperly "mixed and matched" various elements of *Lendenmann* to find it discloses a "first device" specified in claim 1. Specifically, Patent Owner contends the Office and Requester have improperly combined features of the DCE cell, the CDS server, and the RPC server to meet the different limitations regarding the first device. Second Response at 18-19 (citing ACP at 56, 59 and Request at 106-08).

Patent Owner's arguments are based on its misunderstanding of the ACP and the Request. What the cited portions of the ACP and the Request explain is that either the DCE cell or the RPC server may be a "first device" due to the broad language used in claim 1. For example, *Lendenmann* shows that during the RPC binding process, an RPC client uses the name service interface (NSI) to make a request to the appropriate CDS server to get an address associated with a compatible RPC server, which can be identified by a DNS address or an X.500 address. Request at 106-07. The RPC client then sends a request to establish a communications channel to the RPC server in which it can request that security protocols be implemented.

Request at 107-08. Future communications between the RPC client and server are then secure. The first device thus can be either the RPC server or, if the client and server are in different DCE cells, the DCE cell to which the RPC server belongs. Because the RPC server is a part of that DCE cell, any communications sent to or from the RPC server will necessarily be sent to or from the DCE cell. Consequently, any "secure name" associated with the RPC server necessarily is also associated with the DCE cell, so the Office's rejection was proper and should be maintained.

2. Independent Claim 2

The Office correctly found that *Lendenmann* discloses every limitation of dependent claim 2, and thus anticipates this claim. Underpinning this determination was the observation that the systems described in *Lendenmann* can have a variety of configurations and capabilities. Indeed, Patent Owner admits this is the case. *See, e.g.,* First Response at 31-32 ("*Lendenmann*'s DC may include several different components, including security services, time services and directory services. [] It further discloses that a collection of machines, operating systems, and networks managed by a single set of DCE services constitutes a 'DCE cell.' At a minimum, a cell must contain a Security Server, a Cell Directory Server ('CDS'), and Distributed Time Servers. [] These separate components provide different services for establishing remote procedure calls (RPC's) between clients and servers."); *Id.* at 32 ("… *Lendenmann* describes three alternatives [for locating servers that provide services or applications over the DCE]: automatic, implicit or explicit binding. [] A client must then locate servers, for which *Lendenmann* also describes several alternatives: searching files, environment variables, or the CDS; or simply hard-coding a network address into an application.") Patent Owner thus admits that a person of ordinary skill reading *Lendenmann* would have recognized that it is describing not only a wide array of possible configurations of components, but that these different configurations also may exhibit a wide variety of functionalities.

Despite acknowledging the diverse and extensive teachings of *Lendenmann*, Patent Owner disputes that *Lendenmann* anticipates claim 2. Its challenges rest on a distorted reading of *Lendenmann* and an incorrect portrayal of what its claims encompass. Specifically, Patent Owner's arguments are premised on its belief that *Lendenmann* teaches three entirely unrelated models of distributed computing—the client server model, the remote procedure call ("RPC") model, and the data-sharing model—a view contradicted by Patent Owner's own characterizations of *Lendenmann* and by the explicit teachings in *Lendenmann*. Moreover, Patent Owner's assertions rest on a presumption that the claims are limited to specific examples described in the specification of the '181 patent. Patent Owner is incorrect on both points.

a. *Lendenmann* Discloses "Sending a Message to a Secure Name Service," "Receiving a Message Containing the Network Address," and "Sending a Message . . . Using a Secure Communications Link."

In the ACP, the Office correctly found that *Lendenmann* discloses the above-noted claim elements. In its First Response, Patent Owner argued that *Lendenmann* does not disclose "sending a message to a secure name service" and "receiving a message containing the network address." Now, in its Second Response, Patent Owner admits that these limitations are disclosed in *Lendenmann*, but argues that the Office has adopted a "revised argument" that improperly "mixes and matches" various features of *Lendenmann* to satisfy the limitations. *Id.* at 20.

The basis of the Office's rejection of claim 2 has not changed between the First Action and the ACP. In both, the Office and the Requester have relied on the same process, the RPC binding process, to show how the limitations of claim 2 are met. Request at 109-15; First Action at 12-13; ACP at 61-64. For example, in explaining how the elements of claim 2 were satisfied, the Office described a portion of that process—querying the CDS for a network address—that used a client server model. Patent Owner contends this is a new rejection by incorrectly asserting that it combines elements of the client server and RPC models. In reality, the querying process is part of the RPC binding process, as was explained in the Request and the First Action. "The CDS is a secure name service," and it controls access to "'[n]ames in the namespace, including clearinghouses, directories, object entries, softlinks, and child pointers.'" Request at 112-13 (quoting *Lendenmann* at 34). The Request also explained that RPC applications can post and access information on the CDS using the Name Service Interface (NSI): "'Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information.'" Request at 107 (quoting *Lendenmann* at 178-79). The Office also observed in the First Action that this information is used during the RPC binding process, "[w]here the client can utilize the namespace maintained by the CDS for the location of a server that handles the interface that the client is interested in." First Action at 12 (citing *Lendenmann* at 182). Simply put, there is nothing new about the Office's analysis, nor does it rely on a "disjointed" combination of components that are described in *Lendenmann*. Because the Office correctly found that *Lendenmann* discloses "requesting a network address associated with the secure name," "receiving a message containing the network address associated with the secure name," and "sending a message . . . using a secure communications link," the rejection of claim 2 set forth in the ACP was proper and should be maintained.

b. *Lendenmann* Discloses a "Secure Name"

Patent Owner asserts the Office has incorrectly interpreted a "secure name" in a manner inconsistent with the specification. As explained above in the discussion of the basis of the rejection of claim 1, Patent Owner's arguments rest on its belief the claims incorporate limitations shown for specific examples in the specification. The claims do not, as explained above. Moreover, Patent Owner's assertions are inconsistent with its prior representations to the Office as to what a "secure name" may constitute. Consequently, the Office correctly found that *Lendenmann* discloses a "secure name" as that term is used in claim 2.

c. *Lendenmann* Discloses a "Second Device"

Patent Owner argues that the Office has improperly "mixed and matched" various elements of *Lendenmann* to be the "second device" recited in claim 2. According to Patent Owner, the Office and the Requester have asserted that the second device is both the entire DCE cell and a particular server within the cell. Second Response at 22 (citing Request at 111-15). Patent Owner's argument is based on its own misunderstanding of the ACP and the Request. As explained above with respect to claim 1, a "first device" can be <u>either</u> the RPC server <u>or</u>, if the client and server are in different DCE cells, the DCE cell to which the RPC server belongs. Similarly, a "second device" can be <u>either</u> the RPC client <u>or</u>, if the client and server are in different DCE cells, the DCE cell to which the RPC client belongs. Accordingly, *Lendenmann* discloses a "second device" pursuant to claim 2.

d. *Lendenmann* Discloses a "Secure Name Service"

In its First Response, Patent Owner argued that *Lendenmann* does not disclose a "secure name service." First Response at 21-22. The Office responded by explaining that, based on Patent Owner's representations in the prosecution history of the '181 patent and the related '180 patent reexamination, the *Lendenmann* CDS was a "secure name service" within the broadest reasonable construction of that term.

In its Second Response, Patent Owner again argues that *Lendenmann* does not disclose a "secure name service," but now asserts that the Office's construction "contradicts" examples shown in the specification of the '181 patent. This assertion is a red herring – the only "contradiction" that exists at this point is Patent Owner's new interpretation about the '181 specification relative to its prior representations about the same specification. Specifically, in the its earlier representations to the Office, Patent Owner asserted the common specification of the '181 patent compelled the conclusion that a "secure name" was simply a non-standard domain name. And during original examination of the '181 patent, Patent Owner asserted the term could be a "secure name" could be "a secure non-standard domain name" or a "telephone number." First Action (Order) at 5.

There also is no "contradiction" between the Office's definition of "secure name service" and the '181 specification, as Patent Owner contends. Second Request at 23. The example Patent Owner cites from the specification falls within the scope of the Office's construction of "secure name service." Patent Owner's new opinions about the scope of this claim term is, thus, not a "contradiction" but simply a difference of opinion with the Office. If Patent Owner wishes the terms of its claims to have a different scope than what is compelled by the plain language used in those claims, it must amend the claims to correspond to that desired meaning. Because it has not done so, the Office must disregard Patent Owner's arguments that *Lendenmann* does not disclose a "secure name service."

Patent Owner's next criticism can also be dismissed. Patent Owner criticizes the Office's explanation why *Lendenmann* shows a "secure name service" by asserting that the Office has not proven that *Lendenmann* handles X.500 name resolution requests differently than how it handles DNS requests. Patent Owner misses the point – the capacity of the *Lendenmann* systems to act on X.500 names shows that those systems are a "secure name service" within the meaning of the claims. The claims require nothing more. Moreover, there is no requirement in the claims that a system that can function as a "secure name service" cannot also function as an "unsecure" name service. The contrast Patent Owner tries to make can simply be disregarded as it is irrelevant to what has been claimed.

Patent Owner also asserts again that the '181 specification shows that "the standard top-level domain name is replaced with the secure top-level domain name." Second Response at 23. Nothing in claim 2 requires the "replacement" of a "standard top-level domain name" with a "secure top-level domain name." Instead, as the Office found, the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name." Moreover, the Office's construction is consistent with Patent Owner's position during litigation, where it asserted that "Apple server(s) act as a secure name service by storing a network address (*e.g.*, an IP address) associated with the secure name of the of the second device, related to the device's email address or telephone number." Exhibit A at 17-18. The Office thus properly concluded that *Lendenmann* discloses a "secure name service" as specified by claim 2.

e. *Lendenmann* Discloses a "Sending a Message to the Network Address Associated With the Secure Name of the Second Device Using a Secure Communication Link."

The Office correctly found that *Lendenmann* discloses sending a message to the network address associated with a secure name of the second device using a secure communication link. In its Second Response, Patent Owner simply repeats argument it presented in its First Response that no "nexus" exists between security and X.500 names. In the ACP, the Office properly rejected this argument, and it can do so again without further comment. As the Office and the Request each explained, the X.500 name service shown in *Lendenmann* is inherently a secure function because it only is available within a secure network environment. Request at 103-05; ACP at 56, 58. In addition, the claims impose no specific type of connection between the secure name service and the overall functioning of the claimed systems.

Patent Owner also complains that the Office failed to address its prior arguments. This is incorrect; Patent Owner is simply unhappy that the Office found those arguments unpersuasive and did not adopt them. The Office was correct in doing so. For example, in its First Response, Patent Owner sought to read unclaimed limitations from the specification into the claims to prohibit the implementation of any security measures when an "unsecure name" was used. First Response at 39-40. The Office correctly found that the claims imposed no such limitation, and concluded that *Lendenmann* discloses exactly what the claims require: "sending a message to the network address associated with the secure name of the second device using a secure communication link." Patent Owner's attempts to read limitations from the specification into the claims should again be rejected, and the rejection of claim 2 should be maintained.

3. Dependent Claims 5 and 6

The Office correctly found that *Lendenmann* anticipates every limitation of dependent claims 5 and 6. Patent Owner responds that the encryption identified by the Office in the First

Action and ACP do not apply to the messages of claims 5 and 6. Patent Owner is wrong. As the Office found, the CDS is part of *Lendemann*'s security service and the security service provides for encrypted communication between devices. ACP at 65. Thus, *Lendenmann* discloses "receiving the message containing the network address associated with the secure name of the second device . . . in encrypted form" and "decrypting" that message. Accordingly, the Office's rejection of claims 5 and 6 was proper and should be maintained.

4. Dependent Claim 21

The Office properly found that *Lendenmann* describes a system that anticipates claim 21. In response, Patent Owner argues that the "Office's reasoning again has no bearing on the claim" and refers to the arguments made in its First Response. The Office properly disregarded those earlier arguments, as they are unpersuasive. Patent Owner also cites to its prior arguments relating to claim 2, which were unpersuasive and should be disregarded. Accordingly, the Office's rejection of this claim was proper and should be maintained.

5. Independent Claim 24 and Dependent Claim 25

The Office correctly found that *Lendenmann* describes each and every limitation of claims 24 and 25. In response, Patent Owner asserts the rejections should be withdrawn because the Office has used "the same claim interpretation . . . that plague[d] its rejections of claims 1 and 2," referring to the construction of a "secure name" and "unsecure name." Second Response at 25. The Office's interpretation of the claims is neither flawed nor has it changed during the course of the proceeding. Rather, it is the Patent Owner that seeks to improperly limit the scope of the claims by reading unclaimed limitations into them.

Patent Owner also asserts that a "non-final office action is in order" because "what the Office means by 'secure' and 'unsecured,' remain far from settled." *Id.* at 26. There is nothing unsettled about the claim construction the Office has employed – it has remained constant throughout this proceeding. This comment is simply another transparent attempt by Patent Owner to improperly delay these proceedings. As Patent Owner has offered no arguments that would rebut the Office's findings, the rejection of claims 24 and 25 was proper and should be maintained.

6. Independent Claim 26 and Dependent Claim 27

The Examiner correctly found that *Lendenmann* describes each and every limitation of claims 26 and 27. In response, Patent Owner rehashes its arguments from its First Response, asserting that *Lendenmann* does not disclose a server that has a "secure name," an "unsecure name," and a "unique network address." Response at 26-27. Again, Patent Owner's argument rests fundamentally on its desire to incorporate unclaimed limitations into the claims to avoid the prior art.

Here, the claims require registration of an "unsecured name associated with the first device" and "registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name." A device in the *Lendenmann* scheme can be registered with the CDS to be associated with a domain name and also with an X.500 name. This is all that the claims require (*i.e.*, registration with a unsecure and with a secure name). *Lendenmann* also shows that each device has a unique network address, and that the X.500 name is associated with that address. As the Office explained in the ACP, "The X.500 and domain names associated with a device in the *Lendenmann* scheme thus comprise both a unsecure and a unique secure network address. . . . [T]he whole purpose of addressing is for the locating of unique network locations, where *Lendenmann* teaches means for providing naming to network ends where the name corresponds to a specific network address." ACP at 68-69. The Office correctly found that *Lendenmann* discloses all the limitations of claims 26 and 27. Its rejection of those claims was proper and should be maintained.

7. Independent Claims 28 and 29

Patent Owner presents no arguments that are distinct from its arguments provided in response to the rejection of other claims. Because the rejections of those other claims were proper, the rejection of claims 28 and 29 based on *Lendenmann* should be maintained. *See also* Request at 147-160.

8. Dependent Claims 3-9, 12-15, and 18-23

Patent Owner presents no arguments regarding the rejection of claims 3-9, 12-15, and 18-23 based on *Lendenmann* that are distinct from the arguments it provided in response to the rejection of claim 2 over *Lendenmann*. Because the latter rejection was proper, the Examiner's rejection of claim 3-9, 12-15, and 18-23 based on *Lendenmann* is also proper and should be maintained. *See also* Request at 115-130.

F. Response to Patent Owner's Arguments Regarding the Rejection of Claims 10, 11, 16 and 17 Based on *Lendenmann* in view of *Beser* (Issue 7).

The Office properly found that *Lendenmann* in view of *Beser* describes a system that would render obvious claims 10, 11, 16, and 17. In response, Patent Owner asserts simply that *Beser* does not remedy the deficiencies of *Lendenmann*, and refers to its response to the Office's rejection of claim 2 for anticipation by *Lendenmann.* Response at 27. Because the Patent Owner presents no response to the obviousness rejection of claims 10, 11, 16, and 17, that rejection was proper and should be maintained. *See also* Request at 161-163, 164.

G. Response to Patent Owner's Arguments Regarding the Rejection of Claims 10 and 11 Based on *Lendenmann* in view of *RFC 2401* (Issue 8).

The Office properly found that *Lendenmann* in view of *RFC 2401* describes a system that would render obvious claims 10 and 11. In response, Patent Owner asserts only that *RFC 2401* does not remedy the deficiencies of *Lendenmann*, and refers to its response to the Office's rejection of claim 2 for anticipation by *Lendenmann.* Response at 27. Because Patent Owner presents no response to the obviousness rejection of claims 10 and 11, that rejection was proper and should be maintained. *See also* Request at 164-166.

H. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-23 and 28-29 Based on *Provino* (Issue 9).

1. The Office's Rejection of *Provino* Has Remained Consistent

Patent Owner first contends that the Office has "adopted a new rejection" in the ACP. Second Response at 28. Patent Owner's theory is incorrect. Patent Owner omits its assertions in the First Response, which prompted the response of the Office regarding the teachings of Provino. In reality, the manner in which the Request, the First Office Action and the ACP each refer to the disclosure of a "secure name" in *Provino* has remained consistent. For example, the Request, which was incorporated into both the First Office Action and the ACP, explained:

> Provino explains that these DNS systems include secure nameservers (*e.g.*, Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.

Request at 170 (citing *Provino* at 8:67-9:5). Patent Owner ignored this observation in its First Response. This passage shows that a domain name acted on by Nameserver 32 (and which is resolvable into an IP address, *i.e.*, an "integer Internet address") comprises a "secure name" as specified in the '181 patent claims. Thus, the Office has not changed its position on what Provino teaches, much less changed the statutory or substantive basis of the rejections imposed over *Provino*., Instead, it has maintained the same rejection that was previously imposed. *See, e.g.,* Request at 168-171; ACP at 71-73. Patent Owner thus is simply incorrect..

2. Independent Claim 1

In the ACP, the Office correctly maintained its determination that *Provino* anticipates claim 1. In response, Patent Owner asserts the rejection "does not clearly identify the 'First Device' and 'Second Device" of the claim, and that *Provino* does not disclose "a network address corresponding to the secure name associated with the first device," does not disclose the claimed "unsecured name" and is "essentially a Firewall-Based System like those disparaged and disclaimed in the '181 Patent Specification." Second Response at 28-30. Each of these assertions is incorrect, and should be disregarded.

a. Each Rejection Clearly Identifies the First and Second Devices

Patent Owner first asserts that the Request "mixed and matched features from two different devices" in *Provino*, and that Requester has changed its position on which features of *Provino* anticipate the claims. The criticisms levied by Patent Owner are unfounded – Requester's position is unchanged. For example, the Request and First Office Action both pointed out that server 31(S) is the claimed "first device" and "device 12(m)" is the claimed second device in *Provino*. *See, e.g.,* Request at 168-71; First Action at 15-17. Patent Owner's criticisms are simply baseless.

b. Provino Discloses "a Network Address Corresponding to the Secure Name Associated With the First Device"

Patent Owner mischaracterizes the Office's statements regarding "a network address corresponding to the secure name associated with the first device" limitation. Specifically, Patent Owner again incorrectly asserts the Office "now contends that the claimed 'secure name' is 'the integer Internet address' registered with the VPN server of Provino." Second Response at 28-30. This is simply incorrect. As noted above, the Office has consistently explained that the domain names in nameserver 32 of *Provino* constitute the "secure name(s)" disclosed in the '181 patent claims. Thus, as explained in the Request (at 174-175, for example) and the ACP (at 71-73), the "integer Internet address," which is resolvable from the domain name, is the "network address corresponding to the secure name associated with the first device." Patent Owner also contends reading *Provino* in this manner "effectively reads" clauses out of the claims. Petant Owner's assertion rests on its incorrect portrayal of the basis of the rejection and what is shown in *Provino*. It also mischaracterizes the claims, which do not foreclose an integer network address from serving as both the "secure name" and the "network address corresponding to the secure name." Patent Owner's comments, thus, are incorrect and irrelevant to the claims.

c. Provino Discloses an "Unsecured Name"

Patent Owner again contends that *Provino* does not disclose a method for "communicating with a device associated with a secure and an unsecured name…" by asserting the claims exclude the system being described in *Provino*. In particular, Patent Owner claims that nameserver 17 alone "…will not contain any names or addresses associated with [secure nameserver 31(S).." and that "the device 12(m) … will not be able to obtain the integer Internet address of server 31(S) which is accessed from that nameserver 17." Second Response at 29. Patent Owner's comments again incorrectly describe the *Provino* systems and ignores the claim language. First, the claims do not restrict a "device" to a single component shown in the *Provino* systems considered in isolation. Instead, as explained in the Request and the prior actions from the Office, the Provino devices comprise multiple components that interact with each other to provide the functionality specified by the claims. Request at 167-72; First Action at 15-17; ACP at 69-74. Thus, the claims do not require one component in Provino to perform all the functions specified in the claim. Second, in the '181 disclosure, Patent Owner identifies multiple discrete components that interact with each other to provide specified functionalities. *See, e.g.*, Fig. 26 showing DNS server 2609 and DNS Proxy 2610 interacting with "Gate Keeper" 2603 to handle and resolve secure vs. unsecure names. The Office, thus, correctly refuted Patent Owner's incorrect contentions about the capacities and functions of the *Provino* system. *See* ACP at 71-72. Because it has not proposed to amend its claims to exclude the embodiments shown in *Provino,* Patent Owner's arguments must be disregarded.

d. The *Provino* System is Within the Meaning of the Claims of the '181 Patent.

Patent Owner next criticizes the *Provino* scheme, asserting it consists simply of "placing a conventional domain name server behind a firewall" and that this does not "convert it from being conventional into a secure domain name server." Second Response at 30. Patent Owner adds that "a secure domain name server must possess additional functionality not present in a conventional domain name server…" *Id.* Patent Owner concludes that because it "disparaged" conventional domain name servers during prosecution of the '181 patent, the "claims cannot be read to encompass those systems." *Id.* (also citing pages 45-46).

Patent Owner again mischaracterizes both what *Provino* teaches and what its claims encompass. First, *Provino* does not, as Patent Owner contends, consist simply of a conventional name server behind a firewall. Instead, as previously explained, *Provino* shows a system comprising multiple components that work together to receive, at a network address corresponding to a secure name associated with a destination device (*e.g.*, firewall 30, VPN name server 32) a message from a second device to securely communicate. *See, e.g.*, *Provino* at Fig. 1. The routing of a request to that destination where it is evaluated and acted upon is part of the *Provino* system, which means the message will also be received, *inter alia*, by device 12(m) and Name Server 17. If the request specifies a desire to "securely communicate" (*e.g.*, by requesting access to a secure resource within VPN 15 in *Provino*), and the user's credentials are valid, then a VPN is established, and a message (*e.g.*, data for the requested resource) is sent to the requesting entity (the "second device" in claim 1). Moreover, explained in the Request and ACP, the VPN Server 32 is not accessible in the same manner as a conventional domain server. Instead, the *Provino* VPN Server 32 facilitates a secure communication link with authorized devices in the same manner as the "secure name service" described in the '181 patent. Thus, far from being "disparaged and disclaimed," the disclosure of VPN Server 32 in *Provino* is no different than the "secure name service" described by Patent Owner. *Provino*, thus, plainly shows everything required by the claim 1, and therefore anticipates this claim.

Second, the unspecified "additional functionality" Patent Owner refers to is neither identified by it nor is it actually claimed. Instead, the claims by their literal terms encompass the exact systems described in *Provino*. Requester again observes that Patent Owner's "disparagement" theory is factually incorrect and legally irrelevant in this proceeding. For example, the original prosecution history does not show that Patent Owner "disparaged" secure domain name servers such as those shown in *Provino*. In fact, the secure name servers in the '181 specification mirror precisely the *Provino* scheme. In addition, even if Patent Owner had made an effective disclaimer of certain subject matter – which it plainly does not – that disclaimer would only be relevant if it was accompanied by amendment to the claim language that made the claims correspond to that proposed meaning. Since it has not amended the claims, its "disparagement" arguments are legally irrelevant.

3. Independent Claim 2

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of independent claim 2. ACP at 74. In response, Patent Owner presents no response for claim 2 distinct from its response to the rejection of claim 1 over *Provino*. Because the rejection of claim 1 over *Provino* was proper, the Office's rejection of claim 2 over *Provino* also was proper and should be maintained.

4. Claims 3-15, 18-23, and 28-29

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 3-15, 18-23, and 28-29. ACP at 74-75. In response, Patent Owner presents no response for claims 3-15, 18-23 and 28-19 distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 3-15, 18-23, and 28-29 over *Provino* also was proper and should be maintained.

5. Dependent Claim 23

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 23. ACP at 75. In response, Patent Owner presents no response distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 23 over *Provino* also was proper and should be maintained.

6. Independent Claim 28

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 28. ACP at 75. In response, Patent Owner presents no response distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 28 over *Provino* also was proper and should be maintained.

7. Independent Claim 29

In the ACP, the Office correctly maintained its determination that *Provino* discloses every limitation of dependent claim 28. ACP at 75. In response, Patent Owner presents no response distinct from its response to the rejection of claim 2 over *Provino*. Because the rejection of claim 2 over *Provino* was proper, the Office's rejection of claim 1 over on *Provino* also was proper and should be maintained.

I. Response to Patent Owner's Arguments Regarding the Rejection of Claims 24-26 Based on *Provino* in view of *H.323* (Issue 10).

Patent Owner contests the rejection of claims 24-26 as being obvious over *Provino* considered in view of *H.323* without presenting substantive objections to the teachings of either reference. Instead, Patent Owner (i) asserts the Office changed its interpretation of the teachings of *Provino* and this makes it difficult to understand the basis of the rejection, and (ii) disputes that the H.323 properly "incorporates" the teachings of the H.235 publication. Second Response at 31. Neither assertion has any legitimate basis, and each should be disregarded.

First, the basis for the rejection was clearly explained in the Request and the First Action, and has not changed in the ACP. *See* Request at 188-201; First Action at 18; ACP at 75. Patent Owner's assertion that the Office has changed its interpretation of *Provino* and the rejected claims, thus, is incorrect. *See* §H above *Provino*.

Second, the Office properly rejected Patent Owner's "improper incorporation by reference" theory regarding the teachings of *H.323* and *H.235*. *See* ACP at 75-76. As the Office pointed out, *H.323* expressly incorporates *H.235* as "constituting provisions of this [*i.e.*, the *H.323*] Recommendation" (*see* Request at 204 (citing *H.323* at 2-3)) and by stating that "[A]uthentication and security . . . if it is provided, it shall be provided in accordance with Recommendation H.235, Request at 206 (citing *H.323* at 81) (emphasis added). *See also* ACP at 76 ("The Examiner agrees with the third party Requester, H235 is being reference as a standard for security and encryption of H-Series multimedia terminals").

Patent Owner then asserts that it "is not clear how the Office contends the claims are obvious over *Provino* in combination with *H.323* by itself or also in combination with *H.323*." The basis for the rejection of these claims 24-26 is clearly explained in the Request, the First Action and the ACP. Request at 188-201; First Action at 18; ACP at 75. As Patent Owner presents no response specific to the combination of *Provino* with *H.323*, there is no basis for the Office to withdraw its previously imposed rejections, which should be maintained.

J. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-29 Based on *H.323* (Issue 11).

1. Independent Claim 1

In the ACP, the Office maintained its determination that *H.323* describes a system that anticipates claim 1. In response, Patent Owner asserts the same arguments it presented in its First Response, namely that "[c]ombining the teachings of *H.323, H.245, H.235*, and *H.225* is improper," and that *H.323* does not disclose (1) "[a] first device associated with a secure name and an unsecured name," (2) "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device, and (3) "sending a message over a secure communication link from the First Device to the Second Device." Second Response at 32-40. These arguments do not materially change the arguments the Office previously found unpersuasive, and rest on incorrect characterizations of *H.323* and its incorporated teachings.

a. The Teachings of ***H.323***, ***H.245***, ***H.235***, and ***H.225*** Are Properly Combined

In the First Office Action and the ACP, the Office correctly found that *H.245*, *H235* and *H.225* were expressly incorporated into the disclosure of *H.323*, which anticipates claim 1. In its Second Response, Patent Owner again asserts that *H.323* does not properly incorporate the teachings of *H.323, H.245, H.235,* and *H.225* because *H.323* "does not identify with detailed particularity the subject matter" of those references. Second Response at 32-22. Patent Owner is, again, incorrect. First, as explained in the Request, *H.323* expressly incorporates *H.245, H.235,* and *H.245* as "constituting provisions of this [*i.e.*, the *H.323*] Recommendation." Request at 204 (citing *H.323* at 2-3). That is sufficient to incorporate the teachings of *H.245*, *H.235*, and *H.225* in their entirety. *See Harari v. Lee*, 656 F.3d 1331, 1335 (Fed. Cir. 2011) (holding "broad and unequivocal" language sufficient to incorporate the entire disclosure of another reference). Even under stricter standard proposed by Patent Owner, each of *H.245, H.235*, and *H.245* was properly incorporated by reference. For example, *H.323* explains that "authentication and security for H.323 is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235." Request at 204-05 (citing *H.323* at 81 (emphasis added)). Similarly, *H.323* discloses that products claiming compliance with Version 2 of *H.323* shall comply with all of the mandatory requirements of H.323 (1998) which references Recommendations H.225[] (1998) and H.245 (1998)." Request at 205 (citing *H.323* at (i) (emphasis added)). *H.323* also describes *H.225* as containing "[c]all signaling protocols and media stream packetization for packet based multimedia communication systems," and *H.245* as containing "[c]ontrol protocol for multimedia communication." Request at 206-08 (citing *H.323* at 2-3). Each of these statements was identified in the Request, the First Office Action, Requester's comments, and the ACP. Patent Owner continues to ignore these statements in its latest response. Because *H.323* incorporates by reference the teachings of *H.225, H.235*, and *H.245*, the Office's rejection was proper and should be maintained.

Patent Owner also generally argues that, even if the references were properly combined, the Office has "mixed and matched" features from multiple embodiments in *H.323*. Second Response at 31-32. These belated comments should be disregarded as they are not timely. In addition, they should be rejected because Patent Owner does not identify any specific features of *H.323* that were improperly combined. Were the Office to even consider Patent Owner's vague objection, it would be left to guess at which features Patent Owner believes were improperly combined. Finally, Patent Owner's assertions are premised on the mistaken belief that the IPsec protocol cannot be used when an endpoint is protected by a security token. Indeed, *H.323* clearly shows that IPsec is used with security tokens and that IPsec and tokens are part of the same embodiment. Request at 218-26. Because the Office correctly found that *H.323* incorporates the teachings of *H.225, H.235*, and *H.245*, the rejection of the claims over *H.323* were proper and should be maintained.

b. *H.323* Discloses "A First Device Associated With A Secure Name and An Unsecured Name"

The Office correctly determined that *H.323* discloses "a first device associated with a secure name and an unsecured name." ACP at 79-80. In response, Patent Owner again contends that *H.323* does not describe a first device associated with both a "secure name" and an "unsecured name." Second Response at 34-35; First Response at 54. Patent Owner also asserts the Office adopted a new basis for its rejection in the ACP. For the reasons the Office has already conveyed and as set forth below, Patent Owner's contention are incorrect.

First, Patent Owner incorrectly asserts the Office relied on access tokens and the URL of a gatekeeper to satisfy the secure and unsecured names in the First Action, but that in the ACP, relied on "that a 'name and address linked via a registry' correspond to the secure name and unsecure name." Second Response at 34. Patent Owner misunderstands the *H.323* disclosure and the ACP. The ACP did not set forth a new basis for the rejection – the passage referenced by Patent Owner merely refers to a different part of the process described in *H.323* that was identified in the Request and the First Action. Specifically, the Request and the ACP explain that *H.323* discloses that each device in an *H.323* network "is associated with one or more alias names, called Alias addresses, which can be in the form of a phone number or an email address." ACP at 79 (quoting Request at 204). Alias addresses are "secure," in part, because they are "protected by 'access tokens,' which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses." ACP at 79 (quoting Request at 204). The Request also explained that a device will "be[] associated with the unsecured names of the Gatekeeper computer with which they are registered," (Request at 210), and will also "register[] an Access Token instead of a regular Alias address with the Gatekeeper to secure its name and to receive communications at the network address associated with the secure name," (Request at 213).

Patent Owner also complains about the Office's construction of a "secure name" and "secure name registry." Patent Owner's complaint is that the Office has not limited these terms to the examples shown in the specification, or that the Office has disregarded arguments Patent Owner previously made. Patent Owner's criticisms are baseless. Under the Office's broadest reasonable construction policy, a patent owner must amend the claim language to effectively exclude from its scope subject matter literally encompassed by that claim language. *See, e.g.*, M.P.E.P. § 2111.

Requester also notes the Office's construction of these terms as reading on the use of an access token to protect an alias in *H.323* is consistent with Patent Owner's own application of a "secure name" in concurrent litigation against the Requester. In that litigation, Patent Owner contended that Apple's FaceTime "server(s) rely upon a local security certificate on the first Accused Device to secure the name of that device." Exhibit A at 2; *accord id.* at 4. Patent Owner cannot have it both ways. Accordingly, the Office properly determined that *H.323* discloses "a first device associated with a secure name and an unsecured name."

c. *H.323* Discloses "Receiving, at a Network Address Corresponding to the Secure Name Associated With the First Device, A Message From a Second Device of the Desire[] to Securely Communicate With the First Device"

In the ACP, the Office correctly maintained its finding that *H.323* discloses the above claim requirement. ACP at 80-84. In response, Patent Owner offers no new arguments, but simply repeats its baseless assertions regarding the Office's supposed "token-based arguments" and "IPSEC-based rejections." Second Response at 35-39. The Office properly rejected those assertions before, and should do so again. Moreover, Patent Owner mischaracterizes the ACP –

the Office did not impose independent token-based and IPsec-based rejections. As explained above, IPsec is an <u>optional</u> feature that can be implemented <u>along with</u> security tokens. *See* Request at 218-26.

In its challenge to the so-called "token-based" rejections, Patent Owner asserts that none of the devices and messages disclosed in *H.323* corresponds to the "message" or "device[s]" of the claims. Spefically, Patent Owner argues that "[n]one of these messages is sent from the alleged second device (Endpoint A) and 'received, at a network address corresponding to the secure name associated with' the alleged first device (POTS-B). . . . Rather, POTS-B does not receive any message at all in the disclosure of H.235 . . . ." Second Response at 36. Patent Owner's assertions should be disregarded, as the claim language specifies simply that the message be "receiv[ed], <u>at a network address</u> corresponding to the secure name <u>associated</u> with the first device." Patent Owner's argument is thus premised on its mistaken belief that the claims require the message requesting a secure communication link to be received <u>by the first device itself</u> rather than "at a network address corresponding to the secure name associated with the first device." Nothing in the claim language precludes establishment of the secure connection from being mediated by intermediary devices.

Patent Owner's next contention is similarly flawed. Specifically, Patent Owner asserts that the second device does not send a request to securely communicate directly to the first device because the gateway protects that device's addressing information with an access token. Second Response at 36-37. But that assertion is premised on an improper characterization of what the claims actually encompass and ignores that the Office already determined that it is not inconsistent with the claim language for "the gateway [to] act[] and [sic] an intermediary to control access" or for the gateway to "obscure or hide destination addressing information." ACP at 81, 83. This assertion by Patent Owner may therefore be readily dismissed.

Patent Owner's challenge to the purported "IPSec-based" rejections suffer from the same flaws. Here, Patent Owner asserts the messages are "either sent from an endpoint to a gateway, or from a gatekeeper to an endpoint—not from the alleged second device to the first device, as required by the claim." Second Response at 38. Once again, the claim language provides only that the message be "receiv[ed], <u>at a network address</u> corresponding to the secure name <u>associated with the first device.</u>" The Office properly concluded that the secure connection can be mediated by intermediary devices. ACP at 81, 83. *See also* Request at 215-16; ACP at 82-83 (explaining that calling endpoint establishes a channel with the receiving endpoint via a gatekeeper, and the endpoints can negotiate a secure channel either during setup or after the connection has been established). Patent Owner's criticisms can thus be ignored, and the Office should maintain its finding that *H.323* discloses this limitation.

d. *H.323* Discloses "Sending a Message over a Secure Communication Link from the First Device to the Second Device."

The Office correctly maintained its determination that *H.323* discloses "sending a message over a secure communication link from the first device to the second device." ACP at 80-84. In response, Patent Owner argues only that the Office failed to address its arguments in the First Response. Patent Owner is again incorrect. In its prior response, Patent Owner asserted that *H.323* did not show a secure communication link between endpoints. This argument rests on the same, incorrect belief that intermediary devices could not broker a secure communication link. First Response at 58-59. The Office properly rejected that assertion by referring to the actual claim language, and noted Patent Owner had offered no new arguments with respect to the "sending" limitation. ACP 81-84. Consequently, the Office fully addressed and rejected Patent Owner's assertions. The rejection of claim 1 was thus proper and should be maintained.

2. Independent Claim 2

In the ACP, the Office correctly maintained its determination that *H.323* anticipates every limitation of independent claim 2. ACP at 84. In response, Patent Owner repeats the arguments from its First Action, namely that *H.323* fails to disclose (1) "a secure name"; (2) "a network address associated with the secure name of the second device"; (3) "'from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device' and 'at the first device, receiving a message containing the network address associated with the secure name of the second device'"; and (4) "'from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.'" Second Response at 40-44. For the reasons the Office has already conveyed, each of these contentions is incorrect.

a. *H.323* Discloses "A Secure Name"

The Office correctly maintained its determination that *H.323* discloses "a secure name."

In response, Patent Owner presents no response distinct from its response to the rejection of claim 1 over *H.323*. ACP at 84. Because the Office's rejection of claim 1 was proper, its determination that *H.323* discloses the "secure name" of claim 2 was also proper. *See* ACP at 79-80, 84; *see also* Request at 218-226.

b. *H.323* Discloses "A Network Address Associated with the Secure Name of the Second Device"

In the ACP, the Office correctly maintained its determination that *H.323* discloses "a network address associated with the secure name of the second device." ACP at 85-88. In response, Patent Owner repeated its argument that *H.323* does not disclose "a network address associated with the secure name of the second device." Patent Owner's assertion is premised on unclaimed limitations of the claims that would exclude intermediary devices from assisting with establishing a secure connection. The Office properly rejected Patent Owner's assertions when presented previously, and should do so again. ACP at 84-85. The claim language provides only that the "network address" be "<u>associated with</u> the secure name of the second device" and, as the Office found, Patent Owner "attempts to read non-existent limitations into the term 'associated.'" ACP at 86. In the ACP, the Office properly concluded that "the gatekeeper acts and [sic] an intermediary to control access" and "the address of the gateway associated with the second device is sufficient to read on the claim." ACP at 85-86. Accordingly, the Office should maintain its finding that that *H.323* discloses the above limitation.

c. *H.323* Discloses a "'From the First Device, Sending a Message to a Secure Name Service, the Message Requesting a Network Address Associated With the Secure Name of the Second Device' and 'at the First Device, Receiving a Message Containing the Network Address Associated With the Secure Name of the Second Device'"

In the ACP, the Office correctly maintained its determination that *H.323* discloses the above claim requirements. ACP at 85-88. In response, Patent Owner simply repeats the same assertions it made in its First Response. The crux of Patent Owner's position again rests on unclaimed limitations and features of the claims that would prohibit intermediary devices from assisting with establishing a secure connection. For example, Patent Owner asserts that the Office's construction "incorrectly incorporates . . . into the claim . . . [a] third device: the Gateway." Second Response at 42. Similarly, Patent Owner also contends that the security token embodiment cannot read on the claims because "POTS-B has shielded its alleged 'secure name'—the E.164 phone number—from Endpoint A with the security token," and thus, Endpoint A cannot "request[] a name associated with POTS-B's E.164 phone number." Second Response at 42. But the Office has consistently and properly rejected those arguments, explaining that the use of intermediary devices falls within the broadest reasonable construction of the claims. ACP at 85 ("the gateway acts as an intermediary to control access"). Patent Owner also alleges that the Office "pick[s] and choose[s]" features from various unrelated embodiments to satisfy the claims. That assertion rests on the same, incorrect belief that the claims exclude intermediary devices, and therefore the gateway must be considered a first or second device.

d. *H.323* Discloses "From the First Device, Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link"

In the ACP, the Office correctly found that *H.323* discloses "from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link." ACP at 87-88. In response, Patent Owner presents no response distinct from its response to the rejection of claim 1 over *H.323.* Because the Office's rejection of claims 1 was proper, its determination that *H.323* discloses the above limitation of claim 2 also was proper. *See also* Request at 224.

3. Dependent Claims 3-23

In the ACP, the Office correctly found that *H.323* discloses each and every limitation of dependent claims 3-23. ACP at 88. In response, Patent Owner presents no response distinct from its response to the rejection of claims 1 and 2 over *H.323.* Because the rejection of claims 1 and 2 was proper, the Office's rejection of claims 3-23 based on *H.323* also was proper and should be maintained. *See also* Request at 226-242.

4. Dependent Claim 4

In the ACP, the Office correctly maintained its determination that *H.323* anticipates every limitation of dependent claim 4, which provides "the method according to claim 2, wherein the secure name indicates security." ACP at 88. As it did in response to the First Action, Patent Owner contends that the Office "improperly mixed and matched various distinct components of various different references in attempting to meet the claim language." Second Response at 44-

45; *see* First Response at 63. Patent Owner is still incorrect; the only way it can assert that the Office has mixed and matched components is, as explained above for claims 1 and 2, by ignoring the disclosure of *H.323* and misconstring what the claims actually encompass.

Patent Owner also incorrectly asserts that the Requester took a "new position" in its Comments by asserting that the "access token" can satisfy the "wherein the secure name indicate security" limitation of claim 4. Second Response at 44. But the use of the access token was clearly identified in the Request and, in fact, Patent Owner addressed this access token in its own First Response. First Response at 63; Request at 220-23 (explaining how a gatekeeper will recognize the addresses and aliases associated with an access token, "as a 'private' alias, knowing that in order to complete the connection it must return the POTS-gateway address "). Similarly, Patent Owner incorrectly contends that the Office took a new position in the ACP that a "generic name"—a "phone number" or "email address"—corresponds to a secure name. The Office's position is neither new nor different from Requester's. In the ACP, the Office explained that the address of the device corresponding to such an email address or phone number could be protected by an access token. ACP at 79-80. It also found that "access tokens, which obfuscate the destination address information, thus indicate security.'" ACP at 88. The Office's and the Requester's positions are not new, and the Office previously conveyed how the limitations of claim 4 are anticipated by *H.323*. Patent Owner's contentions are simply incorrect.

5. Dependent Claim 5

In the ACP, the Office correctly determined that *H.323* anticipates every limitation of dependent claim 5. ACP at 89. In response to the First Action, Patent Owner argued that *H.323* "fail[s] to disclose 'receiving a message containing the network address associated with the secure name of the second device,' as received in claim 2. For the additional claim 5 feature . . . the address returned in the IPsec passage corresponds to a 'call signaling channel,' rather than the endpoint earlier identified as the 'second device . . . .'" First Response at 63. In the ACP, the Office rejected that argument, observing that Patent Owner had improperly imported <u>unclaimed</u> limitations into claim 2 prohibiting the use of intermediary devices. ACP at 84-85, 89. In its Second Response, Patent Owner presents the same arguments. Because they continue to be based on unclaimed limitations and features of the claims, they should continue to be rejected. In addition, Patent Owner argues the Office has failed to address its arguments relating to the "IPsec embodiment." But, as explained above under claim 2, this argument is based on

Patent Owner's misunderstanding of the H-series processes; IPsec is not a separate embodiment, but an optional feature that can be implemented to work with the security tokens of *H.323*. Accordingly, the Office's rejection of claim 5 over *H.323* was proper and should be maintained.

6. Dependent Claim 9

In the ACP, the Office correctly found that *H.323* anticipates dependent claim 9. ACP at 89-90. In its First Response, Patent Owner asserted simply that "Requester makes the conclusory assertion that any alleged communication link would be initiated automatically." First Response at 64. In response to the ACP, Patent Owner now expands on its assertions, arguing that the literal absence of the words "automatically initiating" in *H.323* means that a secure communication link established would not occur automatically upon completion of negotiation process between networked devices. Second Response at 46. Patent Owner's argument adds nothing new to its previous position, and the Office can reject it on the same basis as it did previously. Patent Owner also incorrectly describes *H.323*. As explained in the Request, First Comments, and ACP, *H.323* explains that "[a]fter obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair." Request at 219. The Office correctly determined these steps occur automatically without any further user interaction. ACP at 90. Accordingly, *H.323* discloses the limitations of claim 9, and the Office's rejection of claim 9 was proper and should be maintained.

7. Dependent Claim 10 and 11

In the ACP, the Office correctly found that *H.323* discloses each of the limitations of claims 10 and 11. ACP at 90. Claim 10 includes the requirement of "receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Claim 11 includes the requirement of "receiving the message in the form of at least one tunneled packet." In response, Patent Owner asserts simply that because it believes *H.323* does not anticipate claim 2, it also fails to anticipate claims dependent from claim 2. As demonstrated above, this assertion is incorrect because claim 2 does not exclude intermediary devices from brokering the secure connection. Consequently, the rejection of claims 10 and 11 was also proper and should be maintained.

8. Dependent Claim 13

In the ACP, the Office correctly found that *H.323* discloses every limitation of claim 13, which specifies that the "receiving and sending of messages through the secure communication link includes multiple sessions." ACP at 91. In its Second Response, Patent Owner makes the same argument it made in its First Response, namely that *H.323* employs separate channels and separate sessions and that claim 13 includes one secure communication link and separate sessions. Second Response at 47; First Response at 64. In the ACP, the Office found that *H.323* provided for the use of multiple sessions and that nothing in the claims limited the multiple sessions to the same secure communication link. ACP at 92. The Office correctly disregarded Patent Owner's incorrect assertions. Accordingly, the rejection was proper and should be maintained.

9. Dependent Claim 21

In the ACP, the Office correctly found that *H.323* anticipates every limitation of dependent claim 21. ACP at 92. In response, Patent Owner presents no response distinct from its response to the rejection of claim 1 over *H.323.* Because the rejection of claim 1 was proper, the Office's rejection of claim 21 based on *H.323* also was proper. *See also* Request at 237-241.

10. Independent Claims 24 and 28 and Dependent Claims 25 and 29

In the ACP, the Office correctly found that *H.323* anticipates every limitation of claims 24, 25, 28, and 29. ACP at 92-93. In response, Patent Owner presents no response distinct from its response to the rejection of claims 1 and 2 over *H.323.* Because the rejection of claims 1 and 2 was proper, the Office's rejection of claims 24, 25, 28, and 29 based on *H.323* also was proper. *See also* Request at 242-48, 258-68.

11. Independent Claim 26 and Dependent Claim 27

In the ACP, the Office correctly maintained its determination that *H.323* anticipates each and every limitation of claims 26 and 27. ACP at 92. In response to the First Action, Patent Owner presented no response distinct from its response to the rejection of claims 1 and 2. In response to the ACP, Patent Owner now complains that the Office did not respond to its argument that *H.323* does not disclose a "unique network address" as required by the claims. Patent Owner is wrong. In confirming the rejections of claims 1 and 2, the Office gave an in-depth explanation of how *H.323* anticipates the claims. ACP at 79-88. In particular, it explained how a gatekeeper in the *H.323* scheme could be associated with one device and how a device could register one secure name and one unsecured name with the gatekeeper, thus satisfying the "unique network address correspond[ing] to the secure name associated with the first device" element of the limitations. ACP at 81-83. The Office's findings also are consistent with Patent Owner's reading of a "unique network address" in concurrent litigation, in which, Patent Owner has asserted "[a] prospective FaceTime caller must also request and obtain registration of a secure name associated with the caller's device through the FaceTime system. . . . [A] certificate assures that the name of the caller's (first) Accused Device is secure. This secure name corresponds to the unique network address of the caller's (first) Accused Device. . . . To call someone using FaceTime, you need their phone number or email address. Exhibit A at 14-15. Thus, because Patent Owner has maintained that an email address or phone number secured by a certificate can "correspond to the unique network address" associated with the first device, its arguments to the contrary should be given no weight by the Office. The Office correctly addressed and dismissed each of Patent Owner's unpersuasive arguments. Accordingly, the Office's rejection of claims 26 and 27 was proper and should be maintained.

K. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-29 Based on *Johnson* in view of *RFC 2131, RFC 1034,* and *RFC 2401* (Issue 13).

1. Independent Claim 1

The Office correctly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claim 1. In response to the ACP, Patent Owner repeats and expands upon arguments it made in its First Response, namely that the references do not teach a system that discloses both "a first device associated with a secure name and an unsecured name." Second Response at 48-52. These arguments can be rejected because they are effectively the same as the arguments in Patent Owner's previous response, which the Office already considered and rejected. Moreover, the arguments are inconsistent with Patent Owner's srepresentations before the Patent Office and should be rejected for that reason.

a. Johnson in view of RFC 2131, RFC 1034 and RFC 2401 Discloses a "a Secure Name" and "a Secure Name Service"

In response to the ACP, Patent Owner states that "the term 'secure name' refers to those names used to communicate securely that are resolved by a secure name service, consistent with its statements during prosecution." Second Response at 49. However, it repeats its arguments that embodiments in the '181 specification additionally require a "secure name server" to "further support establishing a secure communications link" and that *Johnson* discloses a conventional name server that does not. Second Response at 49; First Response at 68. The Office correctly rejected this argument in the ACP, observing that *Johnson*'s secure name server implements security features that make it distinct from a conventional name server. ACP at 95. Also, in the First Action, the Office found that the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name" to distinguish it from a conventional name server. Order at 5. The Office properly rejected Patent Owner's contentions that the claims should be read as implicitly requiring more, in part because those statements are inconsistent with Patent Owner's prior representations to the Office. ACP at 94-95.

Patent Owner also repeats the argument from its First Response that *Johnson* does not disclose a "secure name," asserting that the name used to access *Johnson*'s secure mail server cannot be secure because users know the name in advance. The Office properly addressed and rejected that argument in the ACP, explaining that "the user at the first device requests access to the secure mail server via a 'name' (secure) then when they are authenticated via the secure name service, they are provided with the 'address' (unsecure) corresponding to the provided 'name.'" ACP at 96, 98. The Office correctly observed that the secure name server can require authentication before returning the corresponding network address and the mail server's name can only be resolved by the secure name server; thus the server's name is a "secure name" within the meaning of the claims. The Office thus properly confirmed that *Johnson* discloses the above listed features of claim 1.

b. Johnson in view of RFC 2131, RFC 1034 and RFC 2401 Discloses a "an Unsecured Name"

In response to the ACP, Patent Owner repeats its argument that *Johnson* in view of the other references does not disclose an "unsecured name" because it does not have a domain name registered with the public DNS system. Once again, Patent Owner is wrong. As the Request explained, *Johnson* discloses that the secure name server may be used in many applications, *e.g.*, interbusiness network communication, and it would have been obvious and necessary to register the secure name server with the public DNS system to enable such communications. Request at 272-74. Patent Owner also argues (incorrectly) that the Office changed its position in the ACP to "additionally contend[] that the dynamic address of the secure mail server in Johnson alone corresponds to the 'unsecured name.'" Second Response at 50. The Office has not changed its position. The Request, which the Office incorporated by reference, explained that "the name of the secure mail server is a secure name" and it "has its own unique IP address" as well as "a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an 'unsecured name.'" Request at 274. The Request clearly identified the mail server's address as an unsecured name. Patent Owner's contention this is somehow "new" is thus false. Patent Owner also contends that "an 'Internet protocol address' [is] not a 'name' at all." Second Response at 50. That contention should be disregarded as being inconsistent with Patent Owner's prior representations that distinguish a "secure name" from a conventional name. An IP address, especially one associated with a registered domain name, is a conventional name and it is publicly accessible.

Patent Owner also argues that *Johnson* teaches away from RFC 2131 because *Johnson* "does not rely on any of the[] methods [described in RFC 2131] to assign a dynamic address to the secure mail server." Patent Owner's argument is based on a misreading of *Johnson*. *Johnson* explains "the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network." While Patent Owner contends this teaches away from using DHCP, in fact it does not. Instead, *Johnson* discloses that when the mail server connects to the network, the network <u>assigns it a dynamic address</u> – that is exactly how DHCP works. The Office may thus disregard Patent Owner's contention that "Johnson identifies no DHCP server to convey the address to the secure mail server from the network." Second Response at 51.

Finally, Patent Owner argues that *Johnson*'s intention is to "limit access for security purposes" and it would make little sense for servers of Johnson to register domain names in the public DNS to expand access. However, Patent Owner fails to explain how these purposes are "diametrically opposed" since one of ordinary skill would have appreciated Johnson's intention of developing a flexible system, capable of providing secure communications both within a network and across networks via public resources such as the Internet. The combination does not compromise security or the intended purpose of *Johnson*. Accordingly, the Office properly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claim 1.

2. Independent Claim 2

The Office correctly determined that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious dependent claim 2. Patent Owner presents no response from to its response to claim 1. Accordingly, because its rejection of claim 1 was proper, the Office's rejection of claim 2 also was proper and should be maintained. *See also* Request at 276-282.

3. Dependent Claims 4-6, 8, 12 and 17-20

In the ACP, the Office correctly maintained its determination that *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* renders obvious claims 4-6, 8, 12 and 17-20. In response, Patent Owner presents no response distinct from its response to the rejections of claims 1 and 2. Because the rejections of those claims were proper, the Office's rejections of claims 4-6, 8, 12, and 17-20 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* also were proper and should be maintained. *See also* Request at 284-286, 287-289, 291-292, 294-297.

4. Dependent Claim 3

In the ACP, the Office correctly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered obvious dependent claim 3. In its response to the First Action, Patent Owner asserted that *Johnson* in view of *RFC 1034* failed to disclose an authoritative name server. The Office correctly rejected this argument in the ACP. ACP at 101-02. Now, in response to the ACP, Patent Owner belatedly asserts that *Johnson* in view of *RFC 1034* "does not somehow produce a 'secure domain name'." Second Response at 52-53. The Office should disregard this comment as it is untimely presented. Even if considered, it should be disregarded as being unpersuasive. As the Request explained, a person of ordinary skill in the art would have found motivation within *Johnson* to incorporate mechanisms to facilitate inter-business communications by, for example, making it possible to locate the secure name server 14 by name through the public resources of the Internet. Patent Owner's new argument is based on its misconception that *Johnson* does not show a "secure name" and an "unsecured" name which, as explained above. *See also* Request at 273-74, 282-84. Consequently, the Office's rejection of claim 3 as obvious over *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

5. Dependent Claims 9-11 and 13-16

The Office correctly maintained its determination that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* rendered obvious dependent claims 9-11 and 13-16. In response, Patent Owner presents the same argument the Office rejected in the ACP; namely, that the combination "would change the principle of operation of *Johnson's* system." Second Response at 53; ACP at 103-04. Patent Owner is again incorrect. As explained in the ACP, a person of ordinary skill in the art would have found motivation within *Johnson* to incorporate additional security mechanisms for communications over the Internet, such as interbusiness network communications. ACP at 103-04 (citing Request at 289-90). That person would have found in *Johnson* or *RFC 2401* identification of the same problem (improving security for Internet Protocol communications) as well as a solution to the same problem: an encryption and/or tunneling scheme. There is nothing in either reference that suggests that one must modify the essential features of the *Johnson* systems or change its principle of operation to implement IPSec in communications. Consequently, the Office's rejections of claims 9-11 and 13-16 based on *Johnson* view of *RFC 2131, RFC 1034* and *RFC 2401* was proper and should be maintained.

6. Dependent Claim 21

The Office properly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* would have rendered claim 21 obvious. In response, Patent Owner presents no response distinct from its response to claim 1. Because the rejection of claim 1 was proper, the Office's rejection of claim 21 based on *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* also was proper and should be maintained. *See also* Request at 297-299.

7. Independent Claims 24, 26, 28 and 29

The Office correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render obvious claim 24. In response, Patent Owner presents no response distinct from to its responses to claims 1 and 2. Accordingly, because the Office's rejections of claims 1 and 2 were proper, its rejections of claims 24, 26, 28, and 29 were proper and should be maintained. *See also* Request at 301-304.

8. Dependent Claim 25 and 27

The Office correctly found that *Johnson* in view of *RFC 2131, RFC 1034* and *RFC 2401* describe a system that would render obvious claims 25 and 27. In response, Patent Owner presents no response distinct from to its responses to claims 1, 24, and 26. Accordingly, because the Office's rejections of claims 1, 24, and 26 were proper, the Office's rejections of claims 25 and 27 were proper and should be maintained.

III. There are No Secondary Considerations Linked to the Claims

The Office correctly found no nexus between the putative evidence of secondary considerations presented by Patent Owner and the claimed inventions. ACP 46-48. Its conclusions were correct, given that Patent Owner presented no evidence that any specifically claimed features of the claimed DNS systems could be identified as being attributable to any commercial success of any product or service.

The Office also was correct to not give any weight to the highly biased, self-interested and unsupported testimony of Patent Owner's Chief Technology Officer, Robert Short. Nothing identified by Patent Owner or its uncorroborated witness establishes with a legitimate evidentiary basis that any putative secondary considerations exist that can be attributed to any of the claimed inventions as distinguished from features of products and services known in the prior art, given that claims 1-29 encompass prior art DNS systems.

Finally, evidence of licensing or a jury verdict that is not the subject of a final judgment in concurrent litigation simply is irrelevant – neither constitutes "evidence of commercial success" much less evidence of secondary considerations relevant to the claims. MPEP § 716.03.

For all of the reasons set forth above, Patent Owner has not rebutted the Office's rejections of the claims on any of Issues 1-13, and that nothing raised in Patent Owner's Second Response merits reopening prosecution of the '181 patent. The rejection of all the claims under each of those Issues should, accordingly, be maintained.

Respectfully submitted,

/ Jeffrey P. Kushan /
Reg. No. 43,401
Attorney for Third Party Requester

SIDLEY AUSTIN LLP
1501 K Street, N.W
Washington, D.C. 20005
tel. (202) 736-8000/ fax (202) 736-8711
Date: April 23, 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 05/28/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
05/28/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

VirnetX Inc. : (For Patent Owner)
c/o McDermott Will & Emery :
600 13th Street, N.W. :
Washington, D.C. 20005-3096 :

Sidley Austin LLP : (For Third Party Requester)
717 North Harwood :
Suite 3400 :
Dallas, TX 75201 :

In re Larson :
Inter Partes Reexamination Proceeding : DECISION ON PETITION
Control No.: 95/001,949 :
For U.S. Patent No. 8,051,181 B2 :

This is a decision on a petition filed by the Patent Owner on March 18, 2013 entitled "PATENT OWNER'S PETITION TO REOPEN PROSECUTION" (hereinafter, "the March 18, 2013 petition"). This decision also addresses the Requester's petition, filed on March 27, 2013 entitled "THIRD PARTY REQUESTOR'S PETITION IN OPPOSITION TO PATENT OWNER'S PETITION TO REOPEN PROSECUTION" (hereinafter, "the March 27, 2013 opposition").

These petitions are before the Director of the Central Reexamination Unit for decision.

For the reasons set forth below, the patent owner's petition is denied and the March 27, 2013 opposition is dismissed as moot.

REVIEW OF RELEVANT FACTS

- U.S. Patent No. 8,051,181 issued on November 1, 2011.
- A request for *Inter Partes* reexamination was filed March 28, 2012 and assigned control no. 95/001,949.
- *Inter Partes* reexamination was ordered on June 4, 2012.
- A non-final rejection was mailed on June 4, 2012.
- Patent Owner filed a response to the non-final rejection on September 4, 2012.
- Third Party Requester filed a response after non-final rejection on October 22, 2012.
- An action closing prosecution (ACP) was mailed on January 16, 2013.
- Patent Owner filed a response to the ACP on March 18, 2013.
- Patent Owner filed a petition entitled "PATENT OWNER'S PETITION TO REOPEN PROSECUTION" concurrently with the response filed on March 18, 2013.
- Third Party Requester filed a petition entitled "THIRD PARTY REQUESTOR'S PETITION IN OPPOSITION TO PATENT OWNER'S PETITION TO REOPEN PROSECUTION" on March 27, 2013.
- Third Party Requester filed a response after ACP on April 23, 2013.

STATUTES, REGULATIONS, AND PATENT EXAMINING PROCEDURES

MPEP 2671.02

...it is intended that the second Office action in the reexamination proceeding will ordinarily be an ACP. The criteria for issuing an ACP is analogous to that set forth in MPEP § **706.07**(a) for making a rejection final in an application.

MPEP 706.07(a)

Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims, nor based on information submitted in an information disclosure statement filed during the period set forth in 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p).

MPEP §1207.03(III)

Situations That Are Not Considered As New Grounds of Rejection

There is no new ground of rejection when the basic thrust of the rejection remains the same such that an appellant has been given a fair opportunity to react to the rejection. See *In re Kronig*, 539 F.2d 1300, 1302-03, 190 USPQ 425, 426-27 (CCPA 1976). Where the statutory basis for the rejection remains the same, and the evidence relied upon in support of the rejection remains the same, a change in the discussion of, or rationale in support of, the rejection does not necessarily constitute a new ground of rejection. *Id.* at 1303, 190 USPQ at 427.

DECISION

In the March 18, 2013 petition, the patent owner seeks review of the Examiner's Action Closing Prosecution mailed on January 16, 2013 and requests that the Action Closing Prosecution be deemed premature and prosecution be reopened. The patent owner argues the ACP adopts a new basis for the rejections inconsistent with positions taken in the first Office action, and that prosecution should be reopened to give patent owner a sufficient opportunity to respond to newly adopted positions. See Petition pages 1-2.

Regarding patent owner's argument that the ACP includes new grounds of rejection not necessitated by amendment, it is noted the ultimate criterion of whether a rejection is considered "new" is whether the patent owner had a fair opportunity to respond to the thrust of the rejection. In re Leithem, 100 USPQ 2d 1155, 1158 (Fed. Cir. 2011); In re Kronig, 190 USPQ 425, 426 (CCPA 1976). As stated in MPEP 1207.03(III), "where the statutory basis for the rejection remains the same, and the evidence relied upon in support of the rejection remains the same, a change in the discussion of, or rationale in support of, the rejection does not necessarily constitute a new ground of rejection. *Id.* at 1303, 190 USPQ at 427." Merely providing additional explanation in response to an appellant's argument does not necessarily change the thrust of the rejection. In re Jung, 98 USPQ2d 1174, 1180 (Fed. Cir. 2011).

Upon review, it is noted that the grounds of rejections as presented on pages 4-12 of the ACP are identical to those presented on pages 4-12 of the non-final office action mailed on June

4, 2012. Thus, the rejections in the ACP have not changed when compared to the rejections presented in the non-final office action because the same evidence relied upon and the statutory basis for these rejections has remained the same. Further, all of the portions of the ACP that the patent owner alleges are new rejections are found in the "Response to Arguments" section of the ACP where the examiner has further explained his position to rebut patent owner's arguments. As noted above, merely providing additional explanation in response to arguments does not necessarily change the thrust of the rejection. In re Jung, 98 USPQ2d at 1180.

Specifically, regarding Mattaway, patent owner contends that the Office changed its position in explaining in that the desire to securely communicate is received at the first device in the form of the <CALL> message instead of the <CONNECT REQ> message. However, upon review, the Examiner only provided a response to patent owner's argument that Mattaway did not teach receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire to securely communicate with the first device. The examiner pointed out how the <Connect Req> (the "desire to securely communicate") was indeed received at the first device in the form of a <Call> message. Notably, as pointed out above, the rejection set forth in the "Claim Rejections" section of the ACP did not change. In view of the foregoing, it is determined that the additional explanation of the Mattaway reference provided by the examiner in the ACP does not constitute a new grounds of rejection, which would render the ACP improper.

Second, regarding Provino, patent owner argues the Office changed its position in stating that the "secure name" does not correspond to the "the Domain name stored in the VPN Name Server 32," but instead corresponds to an integer Internet address (ACP at 71). Upon review, this position is consistent with the non-final office action which incorporated page 170 of the Request by reference which states, "Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet address for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." See Provino at 8:67-9:5." Thus, the non-final and the ACP have consistently identified the Domain Name in the Nameserver 32 (which is resolvable into an IP address, i.e. an integer Internet address") as acting on a "secure name". Notably, as pointed out above, the rejection set forth in the "Claim Rejections" section of the ACP did not change. In view of the foregoing, it is determined that the ACP does not present a new grounds of rejection, which would render the ACP improper.

Third, regarding Lendenmann, patent owner argues the Office did not contest patent owner's argument with respect to the RPC model and instead relied on page 21 of Lendenmann as disclosing that Lendenmann's Cell Directory Server (CDS) (which follows the client/server model), when given an X.500 name, returns a network address. Patent owner argues for the first time in the ACP, the office relies on the client/server model of Lendenmann instead of the RPC model. Upon review, it is found that the Office has consistently relied on the blend of the RPC and client server models. See Request at pages 112-114 incorporated by reference in the non-final office action at page 7 and ACP at pages 60-61. Specifically, page 113 of the Request which was incorporated by reference in the non-final office action, states, "Lendenmann teaches a CDS that stores names of resources in that cell so that when given a name, CDS returns the network address of the named resources (see page 21)". Notably, as pointed out above, the rejection set forth in the "Claim Rejections" section of the ACP did not change. In view of the foregoing, it is determined that ACP does not present a new grounds of rejection, which would render the ACP improper.

Fourth, regarding Johnson, patent owner argues the ACP relies on the dynamic address of the secure mail server 16 in Johnson as disclosing the "unsecured name" which is different than the element previously relied upon. The Request at pages 273-274 provided two alternatives as the unsecured name. First, the client identifier for secure name server 14 is an unsecured name. The Request states it would be known to use a domain name registered in the public DNS system and that the publicly registered domain name was an unsecure name (Johnson at column 11, lines 21-37; ACP at 98 and non-final office action at page 12. Notably, as pointed out above, the rejection set forth in the "Claim Rejections" section of the ACP did not change. In view of the foregoing, it is determined that the ACP does not present a new grounds of rejection, which would render the ACP improper.

For the foregoing reasons, the March 18, 2013 petition is denied and the March 27, 2013 opposition is dismissed as moot.

CONCLUSION

1. The March 18, 2013 petition is denied and the March 27, 2013 opposition is dismissed as moot.

2. Telephone inquiries related to this decision should be directed to Alexander Kosowski, at (571)272-3744, Andrew Fischer, at (571) 272-6779, or Sudhanshu Pathak at (571) 272-5509.

Irem Yucel
Director, Central Reexamination Unit

Attorney Docket No. 11798.0013
Control No. 95/001,949

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,949
	)	
U.S. Patent No. 8,051,181	)	Group Art Unit: 3992
	)	
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation Nos. 4522
	)	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

UPDATED NOTICE OF PRIOR AND CONCURRENT PROCEEDINGS

Pursuant to 37 C.F.R. § 1.985, VirnetX Inc., the patent owner, provides this updated notice of prior and concurrent proceedings. U.S. Patent No. 8,051,181 (the '181 patent), which is the subject of this proceeding, is currently at issue in the following litigation:

VirnetX Inc. v. Apple Inc., No. 6:10-cv-00563 (E.D. Tex.).

The '181 patent was previously at issue in the following International Trade Commission investigations that have been terminated:

In the Matter of Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing the Same, Investigation No. 337-TA-818 (Int'l Trade Comm'n); and

In the Matter of Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing the Same, Investigation No. 337-TA-858 (Int'l Trade Comm'n).

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 7, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	15982268
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Pier Douglas DeRoo/Beverly Green
Filer Authorized By:	Pier Douglas DeRoo
Attorney Docket Number:	41484-80200
Receipt Date:	07-JUN-2013
Filing Date:	28-MAR-2012
Time Stamp:	15:48:24
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Miscellaneous Incoming Letter	Litigation_Notice_181_Patent.pdf	63034 6c880c3784151f7404fc6f0ac5d225e2ce70213c	no	2

Warnings:

Information:

Total Files Size (in bytes):	63034

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	Control No.: 95/001,949
Victor Larson et al.	Group Art Unit: 3992
U.S. Patent No. 8,051,181	Examiner: Dennis G. Bonshock
Issued: November 1, 2011	Confirmation No.: 4522
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Updated Notice of Prior and Concurrent Proceedings was served by first-class mail on June 10, 2013, on counsel for third party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 10, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	15996209
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Pier Douglas DeRoo/Sheryl lewissh
Filer Authorized By:	Pier Douglas DeRoo
Attorney Docket Number:	41484-80200
Receipt Date:	10-JUN-2013
Filing Date:	28-MAR-2012
Time Stamp:	16:38:04
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	COS181.pdf	42466 8d29e73bbccab4381fba39c1448c311ae0e1042d	no	1

Warnings:

Information:

Total Files Size (in bytes):	42466

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	16068526
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Karen L. Knezek./Jennifer Gordon
Filer Authorized By:	Karen L. Knezek.
Attorney Docket Number:	41484-80200
Receipt Date:	18-JUN-2013
Filing Date:	28-MAR-2012
Time Stamp:	12:08:20
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Third Party Requester Comments after Action Closing Prosecution	2013_04_23_181_Comments_by_3P_Requester_4.pdf	1639111 e8bcf98fcd4835bbe1e86f9b5bc07e5b78ef7147	no	50

Warnings:

Information:

Total Files Size (in bytes):	1639111

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)
Victor Larson et al.	) Control No.: 95/001,949
U.S. Patent No. 8,051,181	) Group Art Unit: 3992
Issued: November 1, 2011	) Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	) Confirmation No.: 4522
	) VIA EFS WEB

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PETITION SEEKING REVIEW OF DECISION DENYING PATENT OWNER'S PETITION TO REOPEN PROSECUTION

VirnetX Inc. ("VirnetX"), the owner of U.S. Patent No. 8,051,181 ("the '181 patent"), requests that the Director review and overturn the Office's May 28, 2013 Decision on Petition ("Decision"). The Decision improperly dismissed VirnetX's March 18, 2013 Petition to Reopen Prosecution ("Petition"), so VirnetX requests that the Director reopen prosecution.

If entry and consideration of this petition require suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. In addition, if there is any fee due in connection with the filing of this petition, please charge the fee to Deposit Account 06-0916.

I. BACKGROUND

Third-party requester Apple Inc. ("Apple") filed a Request for Reexamination ("Request" or "Req.") on March 28, 2012. The Office granted the Request and issued a first Office Action on June

4, 2012, incorporating by reference nearly all of the Request. VirnetX filed a response ("Response") to the first Office Action on September 4, 2012. Apple filed third-party comments ("Comments") to VirnetX's Response on October 22, 2012. The Office subsequently issued an Action Closing Prosecution ("ACP") on January 16, 2013, maintaining each of the rejections adopted in the first Office Action.

On March 28, 2013, VirnetX petitioned the Office to reopen prosecution. In the Petition, VirnetX explained that the ACP provided new bases for its rejections by, among other things, switching and relying on different features in the references that were not previously relied upon in the initial Office Action. (Petition 2-7.) As one example, VirnetX explained that the ACP included a new rejection of the claims based on *Mattaway* where the Office relied on one message between two particular devices as corresponding to a "message" feature of claim 1 in the initial Office Action, but switched to rely on a different message between different devices to maintain the rejection in the ACP. (*Id.* at 2-4.)

The Office denied VirnetX's Petition in its Decision on May 28, 2013. The Office stated that the *Mattaway* and other rejections in the ACP were not new rejections because the Office employed the same references and the same statutory bases for the rejections. (Decision 3-4.) The Office further reasoned that that there were no actual discrepancies between the office actions because the examiner had simply "further explained his position to rebut patent owner's arguments." (*Id.*) The Office treated its new rejections for *Provino*, *Lendenmann*, and *Johnson* similarly. (*See* Decision at 4-5.)

As explained below, the Office should not have designated the second Office Action an action closing prosecution. Because the Office changed its positions and simultaneously closed prosecution in the same communication, the Office did not afford VirnetX a fair opportunity to respond to the Office's new positions while prosecution was open. Also, by denying VirnetX the opportunity to respond to its new positions while prosecution was open, the Office did not allow a clear issue to develop before closing prosecution. "Before an ACP is in order, a clear issue should be developed." M.P.E.P. § 2671.02; 37 C.F.R. § 1.949. As a result, the ACP was premature.

II. ARGUMENT

VirnetX requests that the Director reverse the previous Decision and reopen prosecution at least because the Decision improperly found that at least the *Mattaway*, *Provino*, and *Johnson* rejections were not new grounds of rejection.[1]

An ACP includes a new ground of rejection if the examiner relies on new facts and rationales not previously raised to the patent owner. *See In re Leithem*, 661 F.3d 1316, 1319 (Fed. Cir. 2011).[2] "Mere reliance . . . on the same type of rejection or the same prior art references . . . is insufficient to avoid a new ground of rejection where [an ACP] propounds new facts and rationales to advance a rejection—none of which were previously raised by the examiner." *In re Stepan Co.*, 660 F.3d 1341, 1345 (Fed. Cir. 2011). Where the Office adopts new theories about prior art references and finds new facts in the references to rely upon in maintaining a rejection, the Office may not characterize the new positions taken in an ACP as "simply an additional explanation." *In re Kumar*, 418 F.3d 1361, 1367 (Fed. Cir. 2005). Rather, "[t]he thrust of the [Office's] rejection changes where, as here, it finds facts not found by the examiner . . . and these facts are the principal evidence upon which the [maintained] rejection was based." *Leithem*, 661 F.3d at 1320 (finding a new ground rejection despite reliance on the same statutory basis and same prior art).

[1] VirnetX continues to disagree with the Office's decision with respect to *Lendenmann*. To expedite resolution of this petition, however, VirnetX is not raising its arguments with respect to *Lendenmann* in this petition.

[2] The Decision cites to cases involving an analogous situation involving determinations of whether the Board has issued a new ground of rejection. VirnetX has done the same here.

A. The Office Adopted a New Rejection Based on *Mattaway*

In the ACP, the Office made new factual findings and advanced new rationales based on *Mattaway* by switching from its reliance on the <CONNECT REQ> message of *Mattaway* in the first Office Action to relying on the <CALL> message of *Mattaway* for the first time in the ACP. (*Compare* ACP 33-34 *with* Req. 70-71, incorporated in Office Action at 5.) These new factual findings and rationales were "the principal evidence" in maintaining the rejection of claim 1. *Leithem*, 661 F.3d at 1320. Accordingly, the "thrust of the rejection" changed in the ACP, and the Office should reconsider its prior Decision and reopen prosecution. *Id.*

In the first Office Action, the Office cited and relied on the <CONNECT REQ> message of *Mattaway* as disclosing the claim 1 feature of "a message . . . of the desire[] to securely communicate." (Req. 70-71; OA 5.) The Office did not cite, mention, or otherwise provide notice of a <CALL> message with respect to this feature of claim 1. (*See id.*)

As *Mattaway* explains, the <CONNECT REQ> and <CALL> messages are different messages sent between different devices. As shown below, a <CONNECT REQ> message (#6) is sent from Webphone 1536 to Global Server 1500, whereas the separate <CALL> message (#8) is sent from Webphone 1536 to Webphone 1538.

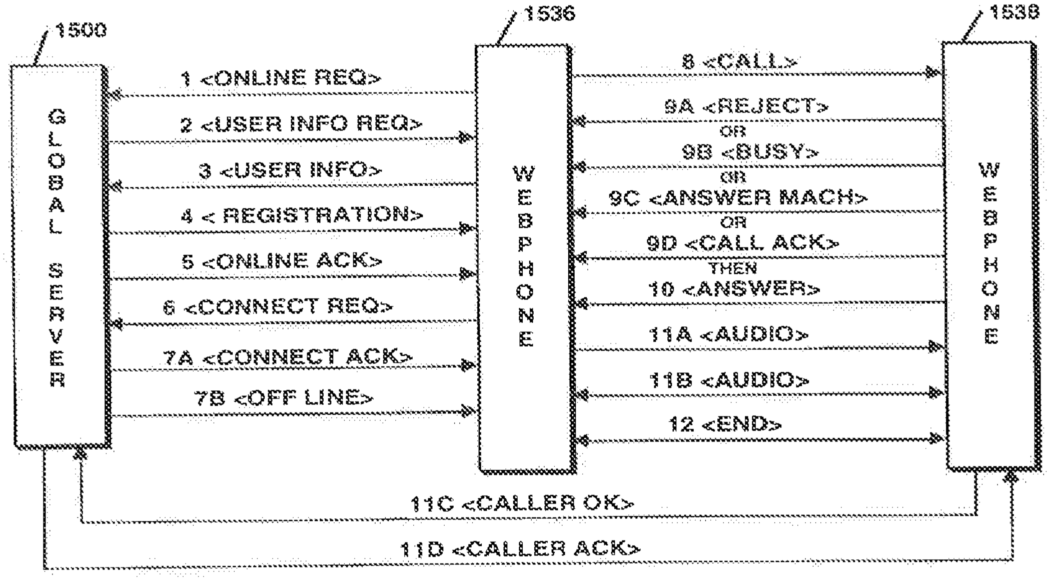


Figure 17A

(*Mattaway* 23:56-59, 24:18-22, discussing Fig. 17A.) The Office disagreed with these teachings of *Mattaway*, contending that a <CONNECT REQ> message may be "received at the first device in the form of a <CALL> message." (Decision 4, emphasis added.) VirnetX disagrees with this assertion, for which the Office provided no citation, (*see id.*), but even if the Office were correct it has still issued a new factual finding that *Mattaway* in some manner teaches messages that change form. This rationale was not advanced in the first Office Action. (*See* Req. 70-71; OA 5.)

In its Response to the first Office Action, VirnetX explained that the <CONNECT REQ> message could not read on the claim feature because, under the Office's proposed arrangement of devices in *Mattaway*, the <CONNECT REQ> message is sent to the wrong device. (*See* Response 21.) The Office did not dispute this argument in its ACP. (ACP 33-34.) Nor did Requester. (Comments 13-14.)

But the Office did not withdraw the rejection. Rather, to rebut Patent Owner's argument and maintain the rejection in the ACP, the Office relied for the first time on the <CALL> message of *Mattaway*, "to which the callee can either <REJECT>, or accept (<CALL ACK>) the call thereby establishing the connection." (ACP 33-34, citing *Mattaway* 24:11-25:34, discussing the <CALL> message.) The new reliance on the <CALL> message is exclusive: in the ACP, the Office no longer cites or mentions the <CONNECT REQ> message. (*Id.*)

The Office's reliance on new factual findings and new features of *Mattaway* changed the thrust of the rejection. *Leithem*, 661 F.3d at 1320. The Office did not identify, discuss, or otherwise mention the <CALL> message in the first Office Action with respect to this "message" feature of claim 1. (*See* Req. at 70-71; OA at 5.) Nor did the first Office Action rely on *Mattaway* as teaching messages that may change form from a <CONNECT REQ> message to a <CALL> message. (*See* Req. at 70-71; OA at 5; *compare* Decision 4.) Accordingly, because the ACP "propound[ed] new facts and rationales to advance a rejection—none of which were previously raised by the examiner," the Office advanced a new ground of rejection. *Stepan*, 660 F.3d at 1345.

The Federal Circuit has held that in circumstances like these, where the Office switches to a different feature or a different interpretation of a reference in maintaining a rejection, prosecution should be reopened. *Leithem*, 661 F.3d at 1320. In *Leithem*, the Office rejected an applicant's claims reciting a "wood fiber pulp" under 35 U.S.C. § 103 based on a prior art reference ("*Novak*") that allegedly taught a "fluff pulp." *Id.* On appeal, the applicant argued that *Novak* did not in fact teach a "fluff pulp," and the Board agreed. *Id.* But the Board did not withdraw the rejection. Instead, the Board maintained the rejection based on *Novak* under § 103 by relying on its finding that the pulp disclosed in *Novak* "may be fluffed." *Id.* The Federal Circuit reversed because the Board improperly "found new facts" based on the prior art in maintaining the rejection, explaining that "Leithem certainly would have responded differently had the examiner's original rejection been premised upon Novak teaching pulp 'which may be fluffed.'" *Id.* Thus, the Federal Circuit remanded to allow "a full opportunity to respond to the new rejection in the first instance." *Id.* at 1321.

The Office should provide such an opportunity to respond here. Contrary to the findings in the Decision, the Examiner did not simply respond to VirnetX's arguments, but rather changed the factual basis of the rejection by relying on the <CALL> message for the first time. (*Compare* Req. 70-71; OA at 5, *with* ACP 33-34.) Specifically, the Office found in the ACP that the <CONNECT REQ> message may allegedly change form, and thereby be "received at the first device in the form of a <CALL> message." (*See* Decision 4). Thus, its interpretation of *Mattaway* and this rationale for the rejection were also the result of new factual findings not raised in the initial Office Action. (*See* Req. 70-71; OA at 5, omitting any discussion of messages changing form.) Either way, the Office advanced a new ground of rejection requiring the reopening of prosecution. *Kumar*, 418 F.3d at 1367 (explaining that it is not "simply an additional explanation" where the Office relies on new factual findings or on a new theory of a prior art reference not earlier raised).

Thus, consistent with Federal Circuit guidance regarding new grounds of rejection, the Office should reconsider its previous Decision and reopen prosecution.

B. The Office Adopted a New Rejection Based on *Provino*

In the ACP, the Office also made new factual findings and advanced new rationales based on *Provino*, and these new facts and rationales were "the principal evidence" in maintaining the rejection of claim 1. *See Leithem*, 661 F.3d at 1320. Accordingly, the "thrust of the rejection" changed for this reason as well, and the Office should reopen prosecution. *Id.*

In the first Office Action, the Office cited *Provino* for the proposition that one particular domain name corresponded to the "secure name" recited in claim 1, while a second domain name corresponded to the "unsecured name" of claim 1. (Req. 168, incorporated in Office Action at 8.)

In response to VirnetX's arguments, the Office ceased relying on these two domain names. (ACP 70-71.) But the Office did not withdraw the rejection in the ACP. Instead, the Office relied for the first time on an "integer Internet address" (instead of an alleged domain name) as corresponding to the "secure name." (*Id.*) This differs from the first Office Action, where the Office did not identify, cite, or otherwise provide notice of an "integer Internet address" as corresponding to the "secure name" feature of claim 1. (*See* Req. at 168-71.)

In the Decision, the Office explained that this discrepancy was not a new rejection because one of *Provino*'s name servers can resolve domain names into integer Internet addresses, as stated in the first Office Action. (Decision 4.) This reasoning is incorrect for similar reasons as those discussed above for *Mattaway*. Just as the first Office Action did not contend the <CONNECT REQ> message of *Mattaway* may change form into a <CALL> message, the first Office Action also did not contend that a domain name in *Provino* may change form into an "integer Internet address" and still qualify as a "secure name." (*See* Req. 168-71; OA 8.) The Office's maintained rejection in the ACP therefore depended on new factual findings regarding *Provino* that were not raised in the initial Office Action, and to which VirnetX has not had an opportunity to respond while prosecution was open. *Stepan*, 660 F.3d at 1345 (the Office advances a new ground of rejection "where [an ACP] propounds new facts and rationales to advance a rejection—none of which were previously raised by the examiner").

The Office cannot close prosecution while allowing elements from prior art references to "change form," yet still reject the '181 patent claims in ways not set forth in the original rejection. *See Leithem*, 661 F.3d at 1320. With *Mattaway* and *Provino*, the Office has made the rejections a moving target, while denying VirnetX an opportunity to respond to the "changed forms" in a nonfinal rejection. This is improper, as "[i]t is crucial that the examiner issue a rejection [in the first instance] . . .so the applicant is on notice that it is obligated to respond." *Stepan*, 660 F.3d at 1344-45.

The Office should accordingly reconsider its prior Decision and reopen prosecution, because the new factual finding based on *Provino*, i.e., that the domain name in *Provino* can change form into a resolved integer IP address and nevertheless still read on the claim, is more than an additional explanation. *Kumar*, 418 F.3d at 1367. This constitutes a new ground of rejection. *Id.*

C. The Office Adopted a New Rejection Based on *Johnson*

The Office also changed the "thrust of the rejection" in the ACP by making new factual findings and advancing new rationales based on *Johnson*.

In its Petition, VirnetX explained that the first Office Action relied on certain specific domain names as corresponding to the "unsecured name" recited in claim 1. (Petition 6-7; *see* Req. 273-74; OA 12.) In response to VirnetX's arguments, the ACP switched features and relied, for the first time, on the "dynamic address of the secure electronic mail server 16" as corresponding to the "unsecured name." (ACP 96.)

In its Decision, the Office explained that the ACP was not inconsistent with the § 103 rejection in the first Office Action because "[t]he Request states it would be known to use a domain name registered in the public DNS system." (Decision 5.) But regardless of whether "it would be known to use a domain name registered in the public DNS system," the Office took the exact opposite position with regards to the "dynamic address of the secure electronic mail server 16" in the first Office Action. It illustrated that the address was not in fact registered in any public DNS system given the security measures dedicating to restricting access to this dynamic address:

> The security of the 'secure name' is further shown 'because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, [such that] *a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16.*'

(Req. 272, quoting *Johnson* 6:25-35.) Because the first Office Action considered it necessary to break through protective encryption measures to obtain the dynamic address, rather than simply looking it up in the public DNS system, the new ACP rejection predicated on obtaining this dynamic address "in the public DNS system" is entirely inconsistent with the first Office Action. (*See* Decision 5.)

Because the ACP adopted a new rejection relying on a reading of *Johnson* entirely at odds with its first Office Action, the Office should reconsider its prior Decision and reopen prosecution. *Leithem*, 661 F.3d at 1320 ("The thrust of the [Office's] rejection changes when, as here, it finds facts not found by the examiner [in the initial rejection] . . . and these facts are the principal evidence upon which the Board's rejection was based.").

III. CONCLUSION

As pointed out in the Decision, the ultimate criterion of whether a rejection is "new" is whether the patent owner has had a fair opportunity to respond to the thrust of the rejection. (Decision 3, citing *Leithem*.) But like in *Leithem*, the Office failed to provide VirnetX with a fair opportunity to respond to at least the *Mattaway*, *Provino*, and *Johnson* rejections because the ACP advanced new rationales and adopted new factual findings based on the prior art references that were not raised in the first Office Action. Just because the Office was responding to VirnetXs arguments when it changed the rejections does not render the new rejections "additional explanation[s]." *Kumar*, 418 F.3d at 1367 (explaining that it is not "simply an additional explanation" where the Office adopts new theories about prior art references and finds new facts in prior art references). Fairness dictates that VirnetX should have an opportunity to respond to the new rejections based on new factual findings with prosecution open, which is in accord with the M.P.E.P. instructions that the Office should liberally grant the reopening of prosecution under these circumstances. M.P.E.P. § 2673.01. Thus, VirnetX respectfully requests that the Director reverse the previous Decision and reopen prosecution.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 9, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
Victor Larson et al.	)	Control No.: 95/001,949
U.S. Patent No. 8,051,181	)	Group Art Unit: 3992
Issued: November 1, 2011	)	Examiner: Dennis G. Bonshock
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK	)	Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Petition Seeking Review of Decision Denying Patent Owner's Petition to Reopen Prosecution was served by first-class mail on July 9, 2013, on counsel for the third-party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 9, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	16263050
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Pier Douglas DeRoo/Sheryl Lewis
Filer Authorized By:	Pier Douglas DeRoo
Attorney Docket Number:	41484-80200
Receipt Date:	09-JUL-2013
Filing Date:	28-MAR-2012
Time Stamp:	15:07:09
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Petition.pdf	567769 c4906e7488c1668b9625b38f49bdd881f24ceb79	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Reexam Miscellaneous Incoming Letter	1	11
	Reexam Certificate of Service	12	12
Warnings:			
Information:			
	Total Files Size (in bytes):	567769	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 07/15/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	PAPER NUMBER
3992	
MAIL DATE	DELIVERY MODE
07/15/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Decision on Petition For Waiver of Page Limit	Control No.: 95/001,949

1. THIS IS A DECISION ON THE PETITION FILED: March 18, 2013.

2. THIS DECISION IS ISSUED PURSUANT TO:

   37 CFR 1.183 — In an extraordinary situation, when justice requires, any requirement of the regulations in this part which is not a requirement of the statutes may be suspended or waived by the Director or the Director's designee, *sua sponte*, or on petition of the interested party, subject to such other requirements as may be imposed.

   37 CFR 1.943(b) — Responses by the patent owner and written comments by the third party requester shall not exceed 50 pages in length, excluding amendments, appendices of claims, and reference materials such as prior art references.

   The petition is before the Office of Patent Legal Administration.

3. RELIEF REQUESTED

   Petitioner requests waiver of the 50-page limit of 37 CFR 1.943(b) for:

   ☒ patent owner's response to the Office action mailed on January 16, 2013.

   □ third party requester comments filed after patent owner's response and the Office action mailed on ____________.

4. FORMAL MATTERS

   a. ☒ Petitioner timely filed a proposed patent owner's response or third party requester comments submission:

      i. ☒ concurrently with the instant petition.

      ii. □ on ____________.

   b. ☒ Petition fee per 37 CFR 1.20(c)(6) was provided.

   c. ☒ Proper certificate of service was provided.

   d. ☒ Petition was properly signed.

5. DECISION (see 37 CFR 1.183 and 1.943(b))

   a. ☒ Granted. Based on the specific facts set forth in the petition under 37 CFR 1.183, petitioner's showing in support of the request for waiver of the 50-page limit of 37 CFR 1.943(b) by attempting to draft a submission in compliance with the 50-page limit and submitting the resulting submission which is in excess of 50 pages, and the individual facts and circumstances of this case, the page limit of 37 CFR 1.943(b) is waived to the extent necessary to permit entry of the submission filed on March 18, 2013. This waiver makes the submission filed on March 18, 2013 page-length compliant.* see attachment.

   b. □ Granted-in-part: see attachment.

   c. □ Dismissed because:

      i. □ Formal matters above. (See unchecked box(es) 4a, b, c, and/or d.)

      ii. □ The petition is unnecessary because the maximum number of pages of the submission filed on ____________ that count toward the regulatory page limit does not exceed 50 pages.

      iii. □ The petition is moot in light of the communication from the Central Reexamination Unit (CRU), mailed on ____________.

      iv. □ Other/comment: see attachment.

6. CONCLUSION

   Telephone inquiries with regard to this decision should be directed to Nicole D. Haines at 571-272-7717. In his/her absence, calls may be directed to Mark Reinhart at 571-272-1611 in the Office of Patent Legal Administration.

/Nicole D. Haines/ Nicole D. Haines [*Signature*]	Senior Legal Advisor [*Title*]

* This decision is limited to the issue of page-length compliance. The Central Reexamination Unit (CRU) will evaluate the submission for compliance with other applicable regulations. Also, this decision does not address the merits of any patent owner requests for entry of amendments and/or evidence pursuant to 37 CFR 1.116, which will be considered by the CRU examiner.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

	)	
In re *Inter Partes* Reexamination of	)	Control No.: 95/001,949
	)	
Patent No. 8,051,181	)	Examiner: Dennis G. Bonshock
	)	
Inventors: Larson et al.	)	Group Art Unit: 3992
	)	
For: METHOD FOR ESTABLISHING	)	Confirmation No.: 4522
SECURE COMMUNICATION LINK	)	
BETWEEN COMPUTERS OF A	)	
VIRTUAL PRIVATE NETWORK	)	

Mail Stop Inter Partes Reexam
ATTN: Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

THIRD PARTY REQUESTER'S OPPOSITION TO PATENT OWNER'S PETITION SEEKING REVIEW OF DECISION DISMISSING PATENT OWNER'S PETITION TO REOPEN PROSECUTION

Third Party Requester Apple Inc. ("Requester") submits these comments in response to Patent Owner's Petition Seeking Review of the Decision Dismissing Patent Owner's Petition to Reopen Prosecution, served by the Patent Owner on July 9, 2013. Requester respectfully requests the Office to dismiss Patent Owner's petition.

I. Relevant Background

On June 12, 2012, the Office commenced *Inter Partes* Reexamination Control No. 95/001,949 (the '949 proceeding) concerning U.S. Patent No. 7,051,181 (the '181 patent) on the basis of a request filed by Apple as a Third Party Requester.

On June 4, 2012, the Office issued an Order ("Order") and Office Action ("First Office Action") imposing rejections on claims 1-29 of the '181 patent.

On September 4, 2012, Patent Owner responded ("First Response") to the Office Action and petitioned the Office to waive the 50-page limit for a Patent Owner response. The response filed by Patent Owner was approximately 115 pages in length.

On October 22, 2012, Requester timely filed written comments on Patent Owner's response to the Office Action. Requester's written comments complied with the 50-page limit specified in 37 CFR 1.943(b).

On December 5, 2012, Third Party Requestor filed a petition to align the schedules of several related proceedings, including Reexamination Control Nos. 95/001,788 and 95/001,189.

On January 16, 2013, the Office issued an Action Closing Prosecution ("ACP") maintaining the rejections previously imposed on all 29 claims of the '181 patent. Each rejection of each claim in the ACP was on the same statutory basis, and relied upon the same prior art, as the corresponding rejection of that claim in the First Office Action.

On January 22, 2013, Patent Owner petitioned the Office for a 1-month extension of the time period for its response, which was granted by the Office on January 25, 2013.

On March 18, 2013, Patent Owner petitioned the Office to Reopen Prosecution alleging that the ACP was premature.

On May 28, 2013, the Office denied Patent Owner's Petition to Reopen Prosecution.

II. Requested Action

Apple requests the Director to dismiss Patent Owner's July 9 petition ("July 9 Petition") in its entirety, as it represents yet another attempt by the Patent Owner to indirectly challenge the merits of the rejections imposed by the Office, and to delay the completion of this reexamination proceeding.

The July 9 Petition alleges that the Office's decision denying Patent Owner's March 18, 2013 Petition to Reopen Prosecution ("March 18 Petition") was improper and requests, once again, to reopen the prosecution. The Office's decision to dismiss the Patent Owner's original petition (the March 18 petition) was proper, and Patent Owner identifies no defect in that decision that merits changing it. As the Office explained in dismissing Patent Owner's March 18 Petition, each of the supposedly "new ground[s] of rejection" the Patent Owner had identified in the March 18 petition (and which it presents again in its latest petition) were not new grounds raised in the ACP, but were the same grounds set forth in the Office's prior rejections or were provided in response to the arguments presented by the Patent Owner in its response to the First Office Action.

On the merits, Patent Owner's July 9 Petition, like its March 18 Petition, misunderstands and mischaracterizes the Office's findings and continues to ignore what is actually shown in the prior art. For the reasons the Office has already conveyed and as set forth below, Patent Owner's contentions are incorrect and should be disregarded.

A. The Office's Rejection Based on *Mattaway* has Remained Consistent

Patent Owner first alleges that, in the ACP, the Office makes "new factual findings and advanced new rationales" in rejecting the claims in view of *Mattaway* and that this means the Office has advanced a "new thrust of rejection." July 9 Petition at 4. Specifically, Patent Owner asserts that in the First Office Action, the Office cited the <CONNECT REQ> message in *Mattaway* as disclosing "a message from a second device of the desire[] to securely communicate with the first device," but in the ACP, the Office changed its position to rely on the <CALL> message. July 9 Petition at 4 (emphasis in original).

Patent Owner is incorrect. The Office's explanation in the ACP directly responds to Patent Owner's baseless criticism of the teachings in *Mattaway*. The Request and the First Action explained that when a caller device wished to securely communicate with a callee device, it would initiate that process by sending a <CONNECT REQ> message, which would result in the "callee" device receiving a message indicating a desire to "directly establish the point-to-point Internet communication with the callee." Request at 71-72; *see also* ACP at 33. In response to the First Action, Patent Owner argued that in *Mattaway* there was no disclosure that the desire to securely communicate was ever "received at a network address corresponding to the secure name associated with the alleged first device." Response at 21. In response, the Requester and the Office each pointed out that the "desire[] to securely communicate" is received at the first device in the form of the <CALL> message, which the callee can decide to accept or reject. Comments at 11-12; ACP at 34 ("the callee receiv[es] a request to communicate from the caller, to which the callee can either <REJECT>, or accept (<CALL ACK>) the call thereby establishing the connection"). This is further confirmed by Figure 17A (which Patent Owner also mischaracterizes), which shows <CALL> as the step (Step 8) following the <CONNECT REQ> and <CONNECT ACK> (Steps 6 and 7A) messages. This is also confirmed by the *Mattaway* specification. *See, e.g., Mattaway* at 23:42-24:42.

Thus, the ACP was simply responding to Patent Owner's baseless and inaccurate criticism of the teachings in *Mattaway*. The Office did not advance a new or changed ground of rejection – it simply responded to Patent Owner's arguments, and demonstrated why it was incorrect. *See* Decision on VirnetX's Petition to Reopen Prosecution ("Decision") at 4.

Undeterred, Patent Owner now asserts that the message transmitted from the second device in *Mattaway* "change[]s form " and "is sent to the wrong device," and that this means the Office's rationale in maintaining the rejection constitutes a new factual finding. July 9 Petition at 5. Patent Owner's attempt to argue the merits of the rejection in a petition should not be tolerated. Moreover, its arguments on the merits of the rejection are baseless. First, nothing in the ACP claims that the <CONNECT REQ> "change[s] form," as Patent Owner contends. Instead, as explained in the Decision, the request to communicate securely message is depicted as being ultimately received by the "second device" as a <CALL> message. Decision at 4. There simply is no finding by the Office that the message "changes form." Second, Patent Owner's contention that the "message" is sent to the wrong device is also incorrect, as nothing in the claim language precludes the message from transmitting through intermediaries, such as the "Global Server" of *Mattaway*. If Patent Owner believes that its claimed "message from a second device" requires direct transmission, it should have sought to amend its claims to require such a step. Nevertheless, the unambiguous language of *Mattaway*, recited by the Examiner in the ACP, explains that the second device may 'directly establish the point-to-point internet communications with the [first device] using the IP address of the [first device].'" ACP at 33 (citing the Request at 72). Patent Owner's inaccurate characterizations of the ACP should be disregarded in considering the present petition.

Patent Owner's reliance on *In re Leithem*, 661 F.3d 1316, 1319 (Fed. Cir. 2011) is misplaced. *Leithem* dealt with a situation where the Board advanced an entirely new obviousness rejection under a rationale not previously advanced by the Examiner —*i.e.*, that the pulp "may be fluffed." *In re Leithem*, 661 F.3d at 1319-20. There is no analogous situation here. First, the Board has not yet considered the findings of the Examiner in this proceeding. Second, in the ACP, the Examiner provided a response to Patent Owner's unpersuasive argument that the <CONNECT REQ> was never received at the second device. The Examiner explained that it was, in fact, received at the second device as evidenced by the <CALL> message. It did not, as Patent Owner contends, impose a new basis of the rejection – the same references were used, and the same statutory grounds employed, to find the claims unpatentable. Accordingly, the Office should dismiss Patent Owner's petition based on its allegations relating to the *Mattaway* reference.

B. The Office's Rejection Based on *Provino* has Remained Consistent

Patent Owner similarly argues that in the ACP the Office "made new factual findings and advanced new rationales based on *Provino*," contending that the Office relied for "the first time" on an "'integer Internet address' (instead of an alleged domain name) as corresponding to the 'secure name." July 9 Petition at 7. Patent Owner's contention is disingenuous as it simply cherry-picks an out-of-context statement from the ACP to support its misguided contention that the Office "did not identify, cite, or otherwise provide notice of an 'integer Internet address' as corresponding to the 'secure name' feature of claim 1. July 9 Petition at 8. In fact, the Request, the First Office Action and the ACP each identify the same feature in *Provino* – the domain name acted upon by Nameserver 32 – as corresponding to the "secure name." The Office's position has remained entirely consistent throughout this reexamination.

The consistent identification of the same "secure name" is exemplified by the explanation in the Request, which was incorporated by the Office into both the First Office Action and the ACP:

> Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." *See* Provino at 8:67-9:5.

Request at 170. The above-quoted language clearly identified the domain name acted upon by Nameserver 32 (which is resolvable into an IP address, i.e., an "integer Internet address") as comprising a "secure name" as specified in the '181 patent claims, and this language was incorporated into both the First Action and the ACP. Patent Owner's decision to ignore this explanation in the Request and First Action when it presented its first response is no basis for reopening prosecution or contending that the Office has altered its factual findings. Thus, the Office has not changed its position at all, but simply maintained the basis of the rejection that had been previously imposed. *See, e.g.*, Request at 168-171; ACP at 71-73. In view of the foregoing, the ACP did not present a new ground of rejection and the Office should disregard Patent Owner's arguments regarding *Provino*.

C. The Office's Rejection Based on *Johnson* has Remained Consistent

Finally, with respect to *Johnson*, Patent Owner alleges the Office "changed the 'thrust of the rejection' in the ACP by making new factual findings and advancing new rationales based on Johnson.'" July 9 Petition at 9. As it incorrectly asserted in the March 18 Petition, Patent Owner again claims the Office has switched the feature in *Johnson* that corresponds to the "unsecure name" recited in the claims of the '181 patent. The Office has not changed its position, and Patent Owner's assertions to the contrary are baseless.

Patent Owner contends that in the First Action, the Office relied on the "dynamic address of the secure mail server 16" as disclosing the claimed "secure name" and that the Office changed its position in the ACP by arguing the same address discloses the claimed "unsecured name." July 9 Petition at 10. This is incorrect. In both the First Action and the ACP, the Examiner found that the dynamic address of the secure mail server in *Johnson* satisfies the "unsecure name" requirement of the relevant claims of the '181 patent. First Action at 20 (citing *Johnson* at 11:21-37); ACP at 98 (citing *Johnson* at 11:21-37). It also found that the publicly registered domain name (the public "address") would be an unsecure name. *Id.* Similarly, in both the First Action and the ACP, the Office found that the name the secure mail server registers with the secure name server is the "secure name." First Action at 20; ACP at 96. Patent Owner's inability to comprehend the clearly disclosed basis for the Examiner's rejections does not mean that the basis of those rejections has changed.

Accordingly, the Director should dismiss the Patent Owner's July 9 Petition to Reopen the Prosecution in its entirety.

The Director is authorized to charge the fee specified in 37 CFR § 1.17(f) to Deposit Account No. 18-1260. In addition, the Director is authorized to charge any other fee he deems necessary to Deposit Account No. 18-1260.

Respectfully submitted,

By:/Jeffrey P. Kushan/ Reg. No. 43,401
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requester

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(202) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile

August 9, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of
U.S. Patent No. 8,051,181
Victor Larson et al.
Issued: November 1, 2011
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949
Group Art Unit: 3992
Examiner: Dennis G. Bonshock
Confirmation No.: 4522

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF SERVICE

I hereby certify that a copy of this correspondence for **Third Party Requester's Opposition to Patent Owner's Petition Seeking Review of Decision Dismissing Patent Owner's Petition to Reopen Prosecution** has been served in its entirety by First Class Mail on the following:

Joseph E. Palys
Finnegan, Henderson, Farabow, Garrett & Dunner LLP
Two Freedom Square
11955 Freedom Drive
Reston, VA 20190-5675

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401
Attorney for Requester

SIDLEY AUSTIN LLP
1501 K Street N.W.
Washington, D.C. 20005
(214) 736-8914 Direct
(202) 736-8000 Main
(202) 736-8711 Facsimile
August 9, 2013

Electronic Acknowledgement Receipt

EFS ID:	16544661
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Karen L. Knezek./Jennifer Gordon
Filer Authorized By:	Karen L. Knezek.
Attorney Docket Number:	41484-80200
Receipt Date:	09-AUG-2013
Filing Date:	28-MAR-2012
Time Stamp:	08:53:20
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam - Opposition filed in response to petition	2013_08_09_3P_Opp_to_PO_Pet_Seek_Review_of_Dec_Dismissing_PO_Pet_to_Reopen_Prosecution.pdf	210524 bb860398a51f06cafba30d4a28c5f563df3c93c4	no	6

Warnings:

Information:

2	Reexam Certificate of Service	2013_08_09_Certificate_of_Service.pdf	127911 2b3dcac5ec5a26a626906b90bf130a0716e10d51	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	338435	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 08/16/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
08/16/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Transmittal of Communication to Third Party Requester *Inter Partes* Reexamination	Control No.	Patent Under Reexamination	
	95/001,949	8051181	
	Examiner	Art Unit	
	DENNIS BONSHOCK	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination prceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Right of Appeal Notice ***(37 CFR 1.953)***	**Control No.** 95/001,949	**Patent Under Reexamination** 8051181
	Examiner DENNIS BONSHOCK	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on 18 March, 2013
Third Party(ies) on 23 April, 2013

Patent owner and/or third party requester(s) may file a notice of appeal with respect to any adverse decision with payment of the fee set forth in 37 CFR 41.20(b)(1) within **one-month or thirty-days (whichever is longer)**. See MPEP 2671. In addition, a party may file a notice of **cross** appeal and pay the 37 CFR 41.20(b)(1) fee **within fourteen days of service** of an opposing party's timely filed notice of appeal. See MPEP 2672.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

If no party timely files a notice of appeal, prosecution on the merits of this reexamination proceeding will be concluded, and the Director of the USPTO will proceed to issue and publish a certificate under 37 CFR 1.997 in accordance with this Office action.

The proposed amendment filed _____ □ will be entered □ will not be entered*

*Reasons for non-entry are given in the body of this notice.

1a. ☒ Claims 1-29 are subject to reexamination.
1b. □ Claims _____ are not subject to reexamination.
2. □ Claims _____ have been cancelled.
3. □ Claims _____ are confirmed. [Unamended patent claims].
4. □ Claims _____ are patentable. [Amended or new claims].
5. ☒ Claims 1-29 are rejected.
6. □ Claims _____ are objected to.
7. □ The drawings filed on _____ □ are acceptable. □ are not acceptable.
8. □ The drawing correction request filed on _____ is □ approved. □ disapproved.
9. □ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d) or (f). The certified copy has:
□ been received. □ not been received. □ been filed in Application/Control No. _____.
10. □ Other _____

Attachments
1. ☒ Notice of References Cited by Examiner, PTO-892
2. □ Information Disclosure Citation, PTO/SB/08
3. □ _____

RIGHT OF APPEAL NOTICE

This action addresses claims 1-29 of United States Patent Number: 8,051,181 (Larson et al.) for which it has been determined in the Order Granting Inter partes Reexamination mailed 6-4-2012 (hereinafter "Order") that a substantial new question of patentability was raised in the Request for *inter partes* reexamination filed on 3-28-2012 (hereinafter "Request").

This is a Right of Appeal Notice in response to the Patent Owner's response filed 3-18-2013 and the Third Party Requester's response filed 4-23-2013.

The Examiner has fully considered this response including the previous court decisions

Claims 1-29 are rejected.

Information Disclosure Statement

No Information Disclosure Statement had been provided by the Patent Owner / 3PR with respect to the 3 provided court papers and the response to the related application. The Examiner has supplemented the file with a PTO-892 entering the references on the record.

Rejections Proposed by the Requester

A total of 12 references have been asserted in the Request as providing teachings relevant to the claims of the Larson patent. In view of the Order, 10 of the proposed issues have established a reasonable likelihood that the Requester will prevail. The following proposed rejections are the main issues to be discussed below:

Issue 1: Claims 1-12 in view of Beser

Issue 3: Claims 1, 2, 6-9, 12, 14-17, 19-21, and 24-29 in view of Mattaway

Issue 4: Claims 3-4, 10-11, 18, and 23 in view of Mattaway in view of Beser

Issue 5: Claims 10 and 11 in view of Mattaway in view of RFC2401

Issue 6: Claims 1-9, 12-15, and 18-29 in view of Lendenmann

Issue 7: Claims 10, 11, and 17 in view of Lendenmann in view of Beser

Issue 8: Claims 10 and 11 in view of Lendenmann in view of RFC2401

Issue 9: Claims 1-15, 18-23, 28, and 29 in view of Provino

Issue 10: Claims 24-26 in view of Provino in view of H.323

Issue 11: Claims 1-29 in view of H.323

Issue 13: Claims 1-16 and 18-29 in view of Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401

Claim Rejection Paragraphs

Claim Rejections - 35 USC § 102

The following are quotations from the MPEP regarding the types of rejections to be utilized below:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Issue 1

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-12, 14, 15, and 17-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-12, 14, 15, and 17-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Beser (see pages 23-40, 41-42, and 43-65 of the Request and pages 1-8 of the Exhibit C1 '181 Patent Claim Charts, incorporated by reference).

Issue 3

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1, 2, 7-9, 12-17, 19-21, and 24-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1, 2, 7-9, 12, 14-17, 19-21, and 24-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Mattaway (see pages 68-94 of the Request and pages 1-8 of Exhibit C2 '181 Patent Claim Charts, incorporated by reference).

Claim 13 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 76 of the Request and pages 4 of Exhibit C2 '181 Patent Claim Charts, incorporated by reference), the Requester lacked a citation to go alone with the quote they cited from the Mattaway reference, which is being herein supplemented by the Examiner.

> *Mattaway discloses that each call, i.e., session, "may be assigned a successive session number in sequence, which may be used by the respective processing unit to associate the call with one of the SLIP/PPP lines, to associate a <ConnectOK> response signal from a <ConnectRequest> signal, and to allow for multiplexing and demultiplexing of inbound and outbound conversations on conference lines .... " (see column 6, lines 24-36)*

Issue 4

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 3-4, 10-11, 18, and 23 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 3-4, 10-11, 18, and 23 are rejected under 35 U.S.C. 103(a) as being obvious over Mattaway in view of Beser (see pages 94-98 of the Request, incorporated by reference).

Issue 5

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10 and 11 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10 and 11 rejected under 35 U.S.C. 103(a) as being obvious over Mattaway in view of RFC2401 (see pages 98-100 in the Request, incorporated by reference).

Issue 6

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-9, 12-15, and 18-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-9, 12-15, and 18-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Lendenmann (see pages 101-159 of the Request and pages 1-7 of Exhibit C3 '181 Patent Claim Charts, incorporated by reference).

Issue 7

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10, 11, and 17 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10, 11, and 17 are rejected under 35 U.S.C. 103(a) as being obvious over Lendenmann in view of Beser (see pages 160-164 of Request, incorporated by reference).

Issue 8

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 10 and 11 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being obvious over Lendenmann in view of RFC 2401 (see pages 164-166 of the Request, incorporated by reference).

Issue 9

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-15, 18-23, 28, and 29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-12, 18-23, 28, and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Provino (see pages 167-203 of the Request and pages 1-8 of Exhibit C4 ‘181 Patent Claim Charts, incorporated by reference).

Claim 13 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 3 of Exhibit C4 ‘181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 1, lines 1-24:

> *The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection there between, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The* ***external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device .***

This paragraph provides support for a plurality of communications being provided during the period when the secure connection channel is enabled.

Claim 14 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 4 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 5, lines 28-35:

> *If the received message packets contain information, such as* ***Web pages or the like****, which is to be displayed to the operator, the information can be provided to the*

> *operator interface 20 to enable the information to be displayed on the device's video display unit.* ***In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.***

This paragraph provides support for a plurality of different services being provided.

Claim 15 is adopted with clarification, as additionally rejected under 35 U.S.C. 102(e) (see page 180 of the Request and pages 4 of Exhibit C4 '181 Patent Claim Charts, incorporated by reference), the Requester lacked an appropriate supporting citation to go alone with the inherency claim made with respect to the Provino reference, which is being herein supplemented by the Examiner.

Provino teaches in column 1, lines 1-24:

> *The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection there between, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The* ***external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device .***

Provino teaches in column 5, lines 28-35:

> *If the received message packets contain information, such as* ***Web pages or the like****, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video*

> *display unit.* ***In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.***

These paragraphs provide support for multiple sessions and a plurality of application programs.

Issue 10

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 24-26 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 24-26 are rejected under 35 U.S.C. 103(a) as being obvious over Provino in view of H.323 (see pages 188-203 of the Request, incorporated by reference).

Issue 11

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-9 and 12-29 are rejected under 35 U.S.C. 102(b) as being obvious over H.323 (see pages 204-268 of the Request and on pages 1-8 of Exhibit C5 '181 Patent Claim Charts, incorporated by reference).

Claims 10 and 11 are adopted with clarification, as additionally rejected under 35 U.S.C. 102(b) (see pages 230-231 of the Request and on page 3 of Exhibit C5 '181 Patent Claim Charts, incorporated by reference)., the Requester lacked an appropriate supporting citation to go alone with the anticipation claim made with respect to the H.323 reference, which is being herein supplemented by the Examiner.

H.323 teaches on page 59:

> ***In order to conserve resources, synchronize call signaling and control, and reduce call setup time, it may be desirable to convey H.245 messages within the Q.931 call signaling channel instead of establishing a separate H.245 channel. This process, known as "encapsulation" or "tunneling" of H.245 messages****, is accomplished by utilizing the h245Control element of h323_uu_pdu on the call signaling channel, copying an encoded H.245 message as an octet string. When tunneling is active, one or more H.245 messages can be encapsulated in any Q.931 message. If tunneling is being utilized and there is no need for transmission of a Q.931 message at the time an H.245 message must be transmitted, then a FACILITY message shall be sent with h323-message-body set to empty.*

This paragraph provides support for tunneling.

Issue 13

This rejection was proposed by the third party requester in the Request, and it is **adopted** with regard to claims 1-16 and 18-29 for the reasons set forth in the Request for reexamination, which is hereby incorporated by reference.

Claims 1-16 and 18-29 are rejected under 35 U.S.C. 103(a) as being obvious over Johnson in conjunction with RFC2131, RFC 1034, and RFC 2401 (see pages 270-318 of the

Request and on pages 1-9 of Exhibit C6 '181 Patent Claim Charts in the Request, incorporated by reference).

RESPONSE TO ARGUMENTS

I. The Rejection of Claims 1-29 Based on Beser (ISSUE 1)

Overview

Beser teaches Unsecure Names / IP addresses of end devices being associated with unique identifiers (such as phone numbers, email addresses, domain name), where this association is made at a third party network device, that provides routing between end devices via the retained list of association. Beser further teaches Secure Names / private IP address of end devices that are packetized so as to translate a packet between end devices where source / destination addresses are of intermediary linking devices (first 14, second 16, trusted third party 30), not the Originating 24 and Terminating 26 devices, who's address is hidden within the packet. (see column 11, line 25 through column 12, line 19, column 10, lines 36-41, and figure 1)

A.

1.

a. Patent Owner (hereinafter PO) argues that "The Office's construction does not even afford the claim terms their plain meaning as it simply ignores entire elements of the claim and the relationship between the claimed first device and second device. Moreover, the Office is also incorrect that the claims merely require "a message" to be sent between two devices at least because the claims clearly recite two different messages (see bullet points 1 and 2 above)."

The Third Party Requestor (hereinafter 3PR) presents "the Office correctly found that Beser shows an originating device (items 24 or 14) (a "second device") that sends a message requesting a connection with a destination device (items 16 or 26) (a "first device") to a trusted third network device. Beser at 11:25-32. The trusted third party network device routes the request to the destination edge router (16) associated with the destination communication device (26) (a "network address corresponding to the secure name associated with the first device"). Id. If the connection is authorized, the trusted third party network device facilitates establishment of a secure communication link between the originating and destination communication devices. Id. Finally, the Office correctly found that Beser discloses that, after the secure link is established, a different message (e.g., packets containing data representing a VOIP communication) is sent from the originating device to the destination device using the secure communication link ("sending a message over a secure communication link from the first device to the second device")."

…

"Beser shows a first message containing a request to communicate with a destination device is sent by the originating device. Beser at Fig. 6. This meets the claim requirement of a "message of the desire to securely communicate" with the destination device. Then, Beser shows that a different message is sent from the trusted third party device to the edge router providing access to the destination communication device which starts the process of negotiation of the secure connection. Id. Beser also shows a different message (e.g., the data representing the content of the VOIP communication) is sent by the originating device to the destination device after the secure connection is established. Id.; id. at 4:44-54. Thus, even under Patent Owner's reading of the claims, Beser plainly anticipates this feature of claim 1."

The Examiner agrees with the third party requestor, the claim merely requires a message, including an IP address, being sent between two devices ("first device"/"second device"). Where the Beser system utilizes an unsecure name (public IP address) to reference another network end, so rather than transmitting a private IP address over the internet, a reference to that end device can be transmitted, and deciphered at an intermediate secure point during transmission, so as to match with the corresponding private IP address, and effect secure communication (see column 11, lines 26 through column 12, line 19). Here, Beser shows an originating device (items 24 or 14) (a "second device") that sends the message to the first device, by first requesting a connection with a destination device (items 16 or 26) (a "first device") via a trusted third network device. Beser at 11:25-3 (this is the first transmission). Then after authentication via this this original request [112], subsequent transmission occurs between devices (second transmission).

b. Patent Owner (hereinafter PO) argues that “the request for reexamination ("Request"), never identified the alleged first device and the alleged second device in Beser. (Response at 9-10.) Instead, the First Office Action incorrectly mixed and matched among four different devices in Beser (first and second network devices 14 and 16 and end- point devices 24 and 26).”… “An anticipation rejection requires that the cited reference disclose all of the claimed features arranged in the way that they are claimed. See M.P.E.P. § 2131. By picking and choosing among different devices in Beser to read on the claimed first and second devices "at any particular point" (Second OA at 17, quoting Comments at 4, emphasis added), the Office and Requester have run afoul of this requirement.”

The Third Party Requestor (hereinafter 3PR) presents “Nothing in the claims precludes a "device" from being an edge router, a communication device or both working in conjunction. In fact, the '181 patent itself illustrates the claimed systems by showing devices on a local network communicating with remote destination using edge routers - precisely what is shown in Beser. Compare Beser at Fig. 1 to ' 181 Patent at 51 : 15-29 and Fig. 28. Patent Owner also disputes the Office's conclusion that the various devices shown in Beser may "at any particular point" qualify as a first or second device. In reality, there is nothing in the claims that precludes reading the claims as encompassing these various embodiments described in Beser. For example, nothing in the claim precludes intermediary devices on a network path from being a first or second "device." And Patent Owner's complaint that the Office and the Request "never identified the alleged first device and the alleged second device in Beecher" is simply false. Second Response at 3."

...

"For example, as explained in the Request, First Action, and ACP, Beser discloses both a "first device" and a "second device" that meet the limitations of the claims. Request at 27-29; First OA at 6-7, ACP at 18-19 (citing Beser at 11:26-12:19). In the Beser systems, when an "originating telephony device" makes a request to securely communicate with a "terminating telephony device," the request is brokered by intermediary devices, including a "first network device," a "second network device," and a "trusted-third-party device." Beser at Fig. 6. The request is a message containing the "unique identifier" for the "terminating telephony device." Beser at 11:25-32. When the "trusted-third- party device" receives the message, it uses the "unique identifier" to look up a public IP address for a "second network device" that is associated with the "terminating telephony device," and then it sends the message requesting a secure connection to the "second network device." Beser at 11:26-32 ("A public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26 at step 116. The second network device 16 is associated with the terminating telephony device 26."). The "second network device" receives the message requesting a secure connection and then negotiates the tunneling association for the "terminating telephony device." Beser at Fig. 6; 11:59-62. The result of the creation of the tunneling associating is that the "terminating telephony device" and the "originating telephony device" (the "first" and "second" devices) can send and receive messages over the secure connection. Thus, contrary to Patent Owner's assertions, the Office and Requester have not been "picking and choosing among different devices in Beser." Instead, they have been comparing what is actually claimed to what is actually disclosed in Beser."

The Examiner agrees with the third party requestor, Beser shows an originating device (items 24 or 14) (a "second device") that sends the message to the first device, by first requesting a connection with a destination device (items 16 or 26) (a "first device") via a trusted third network device. Beser at 11:25-3 (this is the first transmission). As the claims are broadly written, multiple instances of Beser read upon the claims, careful consideration was given to not bonce between elements of Beser to make up a rejection, but rather several individual paths to a complete claim rejection have been provided.

c. Patent Owner (hereinafter PO) argues that "Requester asserts that Patent Owner argued in its Response that the presence and reliance on intermediate devices between the alleged first device and the alleged second device distinguished the claims over Beset. (Comments at 4.) Patent Owner never made this argument and disputes Requester's characterization of Patent Owner's arguments."

The Third Party Requestor (hereinafter 3PR) presents that "Patent Owner misunderstands this point, reading it as suggesting that a single device in tile: Beser system (e.g., one edge router or one communication device) can be both a first and second device. The point made by the Office (and Request) is that either the communication device or the edge router or both working together can be one device within the meaning of the claims. That one device then will communicate securely with a different edge router/commination device/combination (the “second” device).”

The Examiner agrees with the third party requestor, for reasons presented above with respect to a. and b.

2.

a & b.

PO argues that “Beser does not disclose this feature because (1) the broadest reasonable interpretation of "secure communication link" requires encryption, and Beser's tunneling association is not encrypted; and (2) even if the Office maintains that a secure communication link does not require encryption, Beser's tunneling association still is not a secure communication link. (Id. at 10-12.)”

… “Beser also discloses that the addresses of the ends of the tunneling association are "hidden" not using encryption, but instead using the "negotiation" process of step 118 that ensures that the addresses of the ends of the VoIP association are not included in the data packet address fields. (See, e.g., id. at 11:59-12:16; Supp. Keromytis Decl. ¶ 7.)”

… "Accordingly, the portion of Beser that the Office points to as allegedly teaching encryption has nothing to do with the alleged secure communication link and fails to support the rejection."

3PR presents that "passages cited by Patent Owner do not "teach away" from the use of encryption in IP tunneling associations. Rather, what those passages explain is that only in certain high data volume situations can the use of encryption demand additional computational capacity to implement. As was explained in Requester's comments and the ACP, the claims are not limited to high data volume applications, but encompass communications of any magnitude. ACP at 20"

… [pg 8 first par]

… [pg 8 second par]

The Examiner agrees with the third party requestor, to say that Beser's tunneling is not a secure transmission is unfounded, Beser's entire patent is dedicated to creating an alternate and/or supplementary means to encryption for providing secure communication. The method of Beser provides an additional layer of security by not only offering the encryption of data but hiding the source and destination IP addresses (see column 11, line 25 through column 12, line 19).

Beser specifically teaches utilization of encryption in combination with the tunneling, where this tunneling is being used as an additional means of making the channel for transmission secure, yet used in combination with legacy encryption to ensure data security (see column 2, lines 1-16).

B. Independent Claim 2

Patent Owner's argues only for reasons "As discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

C. Dependent Claim 4

PO argues "Dependent claim 4 recites that "the secure name indicates security." Beser does not disclose this feature. The Office and Requester assert that Beser's "unique identifier" discloses a secure name. (Req. at 32.) Beser discloses that the unique identifier may include a dial-up number, e-mail address, domain name, employee number, social security number, driver's license number, previously assigned IP address, etc. (Beser 10:37-11:8.) But none of these examples indicate anything about security."

3PR presents that *"Patent Owner's assertions also are refuted by the teachings of Beser. As explained in the Request, the first network device and the trust-third-party device can recognize the "unique identifier" as being secure and can then implement protocols to obfuscate it from discovery by untrusted parties:*

> *"For each transfer of a packet from the first network device 14 to the trusted- third-party network device 30, the first network device 14 constructs and*

IP 58 packet .... The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12."

Request at 36 (quoting Beser at 11:13-25).

Thus, because Beser recognizes that security must be implemented for certain "unique identifiers," Beser discloses that "the secure name indicates security."

In addition, Beser's "unique identifier" is clearly within the scope of Patent Owner's construction of the term "secure name." As the Office observed in the First Action, Patent Owner asserted during prosecution of the related '180 patent that the term "secure name" could be construed to include "a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number." First Action at 5. Requester has explained that Beser's "unique identifier" could be a non-standard domain name such as a secure domain name or it could be an E. 164 phone number, and the Office has adopted this conclusion. Order at 5-6; Request at 35-36." "

The Examiner agrees with the 3PR, as Beser discloses in the summary that "The method and system described herein may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication without an increased computational burden." This shows the purpose of using alternate names for the network ends it to ensure the security of the communications, not allowing for intermediate data intrusions to recognize the source or destination.

D. Dependent Claim 5

PO argues “Beser does not disclose that the alleged message containing the network address is received in encrypted form. (Response at 13.) The Office and Requester disagree, asserting Beset discloses that "[t]he IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." (Second OA at 23; Comments at 8, both quoting Beser 11:22-25.) This is incorrect because the cited portion of Beset has nothing to do with the alleged message containing the network address.”

3PR presents that “Beser discloses encrypting "IP packets 58 [sic]," which would include any of the packets sent in establishing the secure communications link that contained the "unique identifier," "public IP 58 addresses," or "private IP 58 addresses." ACP at 23. In response to such a query, the third-party-trusted device would return a message containing the "public IP 58 address" associated with the "unique identifier" of the query. Thus, Beser discloses that the message received by the first network device can be encrypted. Accordingly, Beser discloses that "the message containing the network address associated with the secure name of the second device" is "receiv[ed]... in encrypted form."”

The Examiner agrees with the 3PR, as the IP packets 58 that are passed between entities are clearly provide such that they "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network" (where this is the intermediate transmission medium between the two devices.

E. Independent Claims 24, 26, and 29

Patent Owner's argues only “for reasons similar to those discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

F. Independent Claim 28

Patent Owner's argues only “for reasons similar to those discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

G. Dependent Claims 3, 6-12, 14, 15, 17-23, 25, and 27

Patent Owner's argues only “at least the reasons discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

II. The Rejection of Claims 1, 2, 7-9, 12-17, 19-21, and 24-29 Based on Mattaway (Issue 3)

A.

Overview

Mattaway teaches a connection server 26 that maintains a database 34 of callee email addresses and associated IP addresses, so that when a request is made for a connection via a caller, the caller can be connected to the callee via the association stored at the server. (see column 7, lines 20-36)

1.

PO argues “Neither Mattaway's <CONNECT REQ>message nor its <CALL> message discloses "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[ ] to securely communicate with the first device," as recited in claim 1 (emphasis added).”

3PR presents that “The Office properly rejected that theory because nothing in the claim language requires that the messages themselves have "information related to security." The process disclosed in Mattaway "enables the parties to converse in real-time, telephone quality, encrypted communication over the Intemet and other TCP/IP based networks." Mattaway at col.25, 11.32-34; Request at 72; ACP at 34. Therefore, Mattaway discloses a message from the "second device" of the "desire to securely communicate" pursuant to claim 1. This reading of Mattaway is also consistent with Patent Owner's approach in concurrent litigation, where it has asserted that because Apple's "FaceTime calls are encrypted for secure communication.., any request to make a FaceTime call is a request expressing the desire to securely communication using FaceTime." Exhibit A3 at 2. Patent Owner cannot have it both ways, and its assertion that the message itself must "include... information related to security" must be given no weight in view of its contrary assertions on infringement against Requester."

The Examiner agrees with the 3PR, as the communications between the two parties in Mattaway are secure communications, both because of the encryption and because of the hiding of the IP addresses through use of email addresses; and are responsive to a request for the communication session to be established, they are viewed by the Examiner to be within the bounds of a request to securely communicate. Here, a user may use an alias to access the secured data protected under the firewall, where the secured data includes email addresses and IP addressed (see column 4, lines 50-54 and column 17, lines 44-54). Mattaway further shows the email addresses being encrypted email addresses (see 40:27).

PO argues "The Office and Requester cited to two different protocols in Mattaway, and for each protocol focused on the <CONNECT REQ> message as allegedly disclosing the recited "message... of the desire[] to securely communicate." (Req. at 70-71, citing Mattaway 18:41-45 and Fig. 16A as disclosing processing a <CONNNECT REQ> message in the alleged first protocol; Req. at 71, citing Mattaway 8:25-44 as disclosing processing a <CONNNECT REQ> message in the alleged second protocol.) Now, the Second Office Action takes a new position presented for the first time in Apple's Comments on VirnetX's Response, asserting that Mattaway's <CALL> message corresponds to the recited "message... of the desire[ ] to securely communicate." (Second OA at 34, "the process described in column 24, line 11 through

25, line 34, explains the callee receiving a request to communicate[ ] from the caller, to which the callee can either <REJECT>, or accept (<CALL ACK>) the call thereby establishing the connection.") Mattaway 24:11-25:34, as cited by the Office and Requester, deals exclusively with processing the <CALL> message sent between two webphones and has nothing to do with the <CALL ACK> message."

3PR presents that "The explanation provided by the Office in the ACP was plainly in response to Patent Owner's disingenuous criticism of what Mattaway teaches. For example, Patent Owner argued that in Mattaway there was no disclosure that the desire to securely communicate represented by the <CONNECT> message was ever "received at a network address corresponding to the secure name associated with the alleged first device." Response at 21. In response, the Requester (and Office) pointed out that the <CONNECT> message, i.e., the "desire[] to securely communicate," is received at the first device in the form of the <CALL> message. This is confirmed by Figure 17A (which Patent Owner wrongly states stands for the opposite proposition), as <CALL> is shown as the step (Step 8) following the <CONNECT REQ> and <CONNECT> (Steps 6 and 7A) messages identified in the Request. This is also confirmed by the Mattaway specification. Mattaway at 23:42-24:42. Moreover, the Request explained that after receiving the IP address of the first device, the second device may "directly establish the point-to-point Intemet communications with the [first device] using the IP address of the [first device]." Request at 72; ACP at 33-34. Mattaway discloses these "point-to-point Intemet communications" are accomplished by the second device "open[ing] up a socket" to the first device. See Mattaway at col.24, 11.15-30; ACP at 33-34. The second device transmits a "<CALL>" packet to the first device, to which the first device may, among other things, acknowledge or reject the call. Mattaway at col.24, 1.11 - col.25, 1.12; ACP at 33-34. Patent Owner simply ignores this observation in its response.

The Examiner agrees with the 3PR, as the further specification of the rejection was merely to answer the raised by the Patent Owner. Figure 17A lays out the interrelation between the <CONNECT REQ>, <CONNECT ACK>, and <CALL>. It is further noted by the examiner that the claim doesn't require the access of the first device through use of the secure name, only that the first device is associated with the secure name.

2.

PO argues "Mattaway Fails to Disclose "a First Device Associated with a Secure Name and an Unsecured Name""

... "Mattaway does not disclose that the connection server 26 provides any further support for establishing a secure communication link. (Supp. Keromytis Decl. ¶ 10.) Accordingly, its operation is conventional, it is not a "secure name service" in the context of the '181 patent, and the e-mail addresses disclosed in Mattaway are not "secure names." (Id.)"

3PR presents that "Second Response at 11. These assertions can simply be ignored because they are predicated on Patent Owner's belief that the claims incorporate specific requirements regarding the claimed "secure name" which are not actually recited in the claims. As to the first point, the Office properly found that Patent Owner's representations regarding "secure name" here are inconsistent with those it made during prosecution when it told the Patent Office a "secure name" could be "as simple as a telephone number." ACP at 32. Patent Owner's contentions here also are entirely inconsistent with its assertions in concurrent litigation. Specifically, Requester asserted in an action it commenced in the ITC against Requester that:

The secure name of the device is related to the caller's email address or, for Accused iPhones, the caller's telephone number. The Apple servers which facilitate the FaceTime function store a plurality of secure names and associated network addresses. A prospective caller's registration for FaceTime use using an email address or telephone number constitutes a request for registration of a secure name for the Accused Device used by the caller.

Exhibit A at 10 (emphasis added). As to the latter point--that Mattaway's servers are "conventional"--Patent Owner asks the Office to treat its "disclaimer" of conventional servers as an effective claim limitation that excludes subject matter which the language in the claims actually encompasses. See Second Response at 11-12. Because it has not proposed to amend its claims, these efforts to read limitations into them to exclude the embodiment of the "secure name" shown in Mattaway must be rejected."

The Examiner agrees with the 3PR, as the secure name, or in this case the email address is specifically said to be mapped one-to-one to an IP address of an end system (see column 7, lines 25-36 and column 18, lines 41-61), where in Mattaway, a user may use an alias to access the secured data protected under the firewall, where the secured data includes email addresses and IP addressed (see column 4, lines 50-54 and column 17, lines 44-54). Mattaway further shows the email addresses being encrypted email addresses (see 40:27).

PO argues "Second, Mattaway does not disclose that the alleged secure name--the encrypted e-mail address "eemailAddr" entry of Table 9--is associated with the alleged first device. (Id. ¶ 11.)"

3PR presents that "The Office correctly rejected this assertion in the ACP, explaining that "email addresses" are utilized in Mattaway to obtain IP addresses from the connection server, ACP at 31, and that a "user may use an alias to access the secured data under the firewall, where the secured data includes email addresses and IP addresse[s]." ACP at 32. The devices shown in Mattaway (webphones) are each required to register information as part of the <USER> message. Mattaway 22:65-23:5, 40:27. Mattaway thus discloses that information requested from the first device/Webphone client would include an encrypted email address."

The Examiner agrees with the 3PR, as the email address is specifically said to be mapped one-to-one to an IP address of an end system (see column 7, lines 25-36 and column 18, lines 41-61), where Mattaway describes it as the "E-mail address of the callee".

B. Independent Claim 2

Patent Owner's argues only “for the reasons discussed in the response and those discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

C. Independent Claims 24, 26, 28, and 29

Patent Owner's argues only “for reasons similar to those discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

D. Dependent Claims 7-9, 12-17, 19-21, 25, and 27

Patent Owner's argues only “for at least the reasons discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

III. The Rejection of Claims 3, 4, 10, 11, 18, and 23 under Mattaway and Beser (ISSUE 4)

A. Dependent Claim 4

PO argues “Claim 4 recites that "the secure name indicates security." The combination of Mattaway and Beser does not disclose or suggest this feature. Mattaway does not disclose this feature, and the Office and Requester do not allege that it does. (Req. at 96.) Instead, the Office and Requester allege that Beser discloses this feature, citing the same portion of Beser used to reject claim 4 in the anticipation rejection of

Issue 1. (Id.) This is incorrect because Beser does not disclose that its unique identifier indicates security."

3PR presents that Beser plainly teaches that its scheme - in which the unique identifier plays a critical role - provides security, inter alia, through obsfucation of internal IP addresses of the originating and destination communication devices. See Request at 96. A person of ordinary skill in the art would have plainly recognized from that description that the unique identifier is associated with secure communications.

The Examiner agrees with the 3PR, as Beser discloses in the summary that "The method and system described herein may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication without an increased computational burden." This shows the purpose of using alternate names for the network ends it to ensure the security of the communications, not allowing for intermediate data intrusions to recognize the source or destination.

PO argues "the Office's and Requester's obviousness analysis is deficient because it is based on nothing more than conclusory statements."

3PR presents that "Patent Owner contests for the first time the substantive findings set forth in the First Action regarding Mattaway in view of Beser, contrary to the requirements of 37 C.F.R. 1.951. See 37 C.F.R. 1.951 ("the patent owner may once file comments limited to the issues raised in the Office action closing prosecution.") Patent Owner's belated response should be disregarded."

…

"the Office did not rely on "conclusory" statements to support the rejection of claim 4. Second Response at 13. Instead, as explained in the Request, Mattaway recognizes the importance of using encrypted communications in its system to secure the data that is exchanged. Request at 96. Beser also recognized the importance of securing the data being transmitted in its system, and explained that a further measure of security could be achieved through obfuscation of the unique identifier, i.e., the "secure name" of Beser. Request at 96. Thus, the Request explained in detail why a person of ordinary skill would have considered it obvious to use the obfuscation techniques described in Beser in which the unique identifier "indicates security" in the Mattaway's scheme, which, like Beser, emphasizes security."

The Examiner agrees with the 3PR, the systems are in the same art areas as both systems utilized alternate location naming to locate a remote system through a hidden IP address. Beser merely further provides the reasoning for doing so.

B. Dependent Claim 10

PO argues "he Office asserts that a message in Mattaway from connection server 26 to the first processing unit 12 is the claimed "message containing the network address." (First OA at 5, incorporating Req. at 68-94; Req. at 90.) But, as explained in the Response, this message is not received through the alleged secure communication link, because the Office and Requester assert that the secure communication link is a point-to-point communication between the WebPhone applications of first processing unit 12 and second processing unit 22. (Response at 29; Req. at 90.) Thus, even if Beser's tunneling methods were combined with Mattaway's system as proposed by the Office and Requester, the combination still would not disclose receiving the message "through tunneling within the secure communication link" (emphasis added), because that message is not sent through the alleged secure communication link in the first place."

3PR presents that "a person of ordinary skill in the art would have found motivation within Mattaway to modify the encrypted communications disclosed therein to incorporate additional mechanisms of protection in order to provide a more secure communication link. Request at 96-97; ACP at 51-53. That person would have found that Beser identified the same problem (improving security of network communications) and provided a solution to that problem; namely, to use a particular type of IP tunneling."

The Examiner agrees with the 3PR, as the communication between the server and the first processing unit is part of the overall communication path between the first processing unit and the second processing unit.

C. Dependent Claims 3, 11, 18, and 23

Patent Owner's argues only “for at least the reasons discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

IV. The Rejection of Claims 10 and 11 based on Mattaway and RFC 2401 (ISSUE 5)

A. Dependent Claim 10

PO argues “this message is not received through the alleged secure communication link, because the Office and Requester assert that the secure communication link is a point-to-point communication between the WebPhone applications of first processing unit 12 and second processing unit 22. (Response at 31; Req. at 90.) Thus, even if RFC 2401's tunneling methods were combined with Mattaway's system as proposed by the Office and Requester, the combination still would not disclose receiving the message "through tunneling within the secure communication link" (emphasis added), because that message is not sent through the alleged secure communication link in the first place.”

3PR presents that “a person of ordinary skill in the art would have found motivation within Mattaway to modify the encrypted communications disclosed therein to incorporate additional mechanisms of protection in order to provide a more secure communication link. Request at 98-99; ACP at 54-55. That person also would have recognized that RFC 2401 addresses the same problem - improving security of networked communications - and provides a solution to that problem; namely, use of a particular type of tunneling.

Again, Patent Owner's belated comments should be disregarded as they were not presented in response to this ground of rejection when it was imposed in the First Office Action. They also should be rejected as being incorrect. Indeed, Patent Owner assertions are premised on the mistaken belief that the secure communication link disclosed in Mattaway could not include a communication link with the server that facilitates the secure communication link." Nothing in the description of Mattaway precludes such a configuration."

The Examiner agrees with the 3PR, as again the communication between the server and the web phone is part of the overall secure communication link.

B. Dependent Claim 11

Patent Owner's argues only "for at least the reasons discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

V. Rejections over Lendenmann/Beser/RFC2401 (ISSUES 6-8)

Overview

Lendenmann teaches a Cell Directory Service (CDS) that stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource. (see page 21) Where the client can utilize the namespace maintained by the CDS for the location of a server that handles the interface that the client is interested in (see page 182). Lendenmann further teaches the DCE Naming Service that allows user to identify, by name, resources such as servers, files, disks, or print queues, and gain access to them without needing to know where they are located in a network. (see page 22) Lendenmann further allows for cell name aliasing so as to have a primary name, and one or more alias names that are recognized by DCE services (see page 24). This dual name scheme in Lendenamann provides two naming schemes:

- CCITT X.500 [secure]
- Intemet Domain Name Service (DNS) [not secure]

The DNS naming scheme has "global addressing and routing" and "makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries." Alternatively, the CCITT X.500 naming scheme is a secure, internal naming convention. "The X.500 naming scheme is independent from the Internet and more general. It is implemented with the Global Directory Service (GDS), which can store any kind of object. DCE uses GDS to store cell names and their addresses, which today are also Internet addresses." An example of an X.500 name is: [Cell name] [CDS name]. (see page 23)

A.

1.

a.

(i) Interpreting “Secure Name” and “Unsecured Name”

PO argues “Requester contends that a secure name should be defined by no more than whether it is stored in a secure name registry, and whether a conventional

DNS can resolve it. (Id. at 57-58.) Requester reaches this conclusion solely by relying on the '181 patent prosecution history and a prior reexamination of the '180 patent, without considering the context of the specification itself. (Id.) The Office appears to agree. (Second OA at 58.) The result of Requester's incorrect analysis, however, is an implicit claim construction that removes all meaning of "secure" and "unsecured" from the claim terms. This claim construction also contradicts the portions of the '181 patent specification on which statements from the prosecution history and the prior reexamination were based. The rejections predicated on this deficient construction should be withdrawn."

…

"Requester's out-of-context interpretation of the statements from the '180 patent reexamination contradicts the embodiments in the specification on which the statements from the '180 patent reexamination are based. (See Order at 5, citing '180 patent 51:25-35, corresponding to '181 patent 50:15-25.) These embodiments, relating to Figure 34, describe using a secure domain name for establishing secure communication links, while using unsecured names for non-secure communications. ('181 patent 48:50-52:58.) As just one example, the '181 patent specification describes replacing a top-level domain name with a secure domain name in order to establish a secure communication link. (Id. at 48:53-55, 50:7-59.) Afterwards, the '181 patent specification describes replacing the secure domain name with a non-secure domain name when the secure communication link is terminated. (Id. at 51:51-55.) Requester, by taking the prosecution history and prior reexamination statements out of their context, generates a strained and deficient claim interpretation that strips all plain meaning from the "secure" and "unsecured" claim terms and contradicts the ' 181 patent specification. M.P.E.P. § 2258(I)(G).

The rejection should be withdrawn because Lendenmann, under a reasonable claim interpretation properly reflecting the nexus between secure names and secure communications, does not disclose at least "a first device associated with a secure name and an unsecured name," as recited in claim 1. Indeed, Requester expressly admits that it is "fundamentally implausible" that a name qualifying as a "secure name" would not have any nexus with ensuring secure communications. (Comments at 23.) But the Office and Requester did not dispute that Lendenmann merely presents X.500 and DNS as alternative DCE-compatible naming schemes: "X.500 is an emerging global directory service standard, but the Internet domain name system (DNS) is an established industry standard. For interoperability purposes, GDS supports both X.500 and DNS transparently." (Lendenmann 21; Response at 33; Second OA at 56-58.) As detailed in Patent Owner's previous Response, X.500 and DNS perform the very same functions in Lendenmann's distributed computing environment, and a separate Security Service facilitates security functions without regard to whether a X.500 or DNS name is employed. (Response at 33-35.) Neither the Office nor Requester relies on any Lendenmann passages or provide any other support reflecting any nexus between X.500 names and secure communications. (Second OA at 57-58; Comments at 20-21, 23.)

3PR presents that “As explained in the First Action and ACP, Patent Owner represented to the Office that a "secure name" may be any type of non-standard name. Under that interpretation, a "secure name" may be an X.500 name. ACP at 56; Request at 22; Order at 5 (Patent Owner asserted terms are not indefinite because a "secure name" could be "a secure non-standard domain name" or a "telephone number."). In response, Patent Owner asks the Office to disregard its previous representations that were made to secure allowance of these claims and analogous statements made during reexamination in the ' 180 patent, and instead import restrictions into the claims from particular examples in its specification. For example, Patent Owner contends that its prior statement that a "secure name" could be "a secure non-standard domain name" or a "telephone number" should be ignored because that statement "merely illustrate[s] exemplary differences between a 'secure name' and a 'secure domain name' in response to an indefiniteness rejection." Second Response at 16.”

…

“Patent Owner's statements were not limited as it contends. Rather, Patent Owner asserted that the term was not indefinite because one would recognize it could encompass "a secure non-standard domain name" or a "telephone number." The Office correctly found that because a X.500 name is a "non-standard domain name," it is a "secure name" within the meaning of the claims.”

…

The meanings for these terms that Patent Owner advanced previously to the Office are not incompatible with the claim language. For example, claim 1 uses the term "secure name" to identify the destination of a message. See claim 1 ("receiving, at a network address corresponding to the secure name associated with a first device, a message from a second device"). Similarly, in claim 2, the term is used to identify a device. See claim 2 ("from the first device, sending a message to a secure name service, the message requesting a network address associated with a secure name of the second device..."). The use of "unsecure" or "secure" names to serve these identification functions is not incompatible with the claim language. In fact, Patent Owner actually uses the precise meaning it advanced during the prior proceedings in a dependent claim. Specifically, claim 23, which depends from claim 2, specifies that a "the secure name of the second device is a secure, non-standard domain name.") Thus, Patent Owner's assertions that the meanings used by the Office and in the Request for "unsecure" and "secure" names are somehow incompatible with its disclosure are simply false."

…

"Patent Owner's arguments thus can be easily dismissed - they do not compare what is actually claimed to the prior art, but instead compare unclaimed features in the specification to the disclosure in Lendenmann."

The Examiner agrees with the 3PR, as previous prosecution history revealed what the terms have been realized to mean, where further guidance and support for the offices/3PRs reading can be seen from EXHIBIT A/13. In EXHIBIT A/13, which was supplied by the Patent Owner to show infringement of accused IOS devices on the '181 Patent, shows on page 3, how a user's selection of a destinations phone number or email address can be utilized as a secure name for contacting a destination party. Here, the Office should consider the Patent Owner's infringement contentions as Patent Owner admissions regarding claim construction in the reexamination proceedings. The mere fact that an alternate embodiment exists in the specification loosely tied to similar language is not persuasive enough to change the way the claim terms have been perceived all along. Utilizing the further guidance provided in the dependent claims (claims 23) the embodiment the claims are directed toward can clearly be distinguished from the meaning the Patent Owner is now attempting to impart on the claims.

PO argues “The rejection should be withdrawn because Lendenmann, under a reasonable claim interpretation properly reflecting the nexus between secure names and secure communications, does not disclose at least "a first device associated with a secure name and an unsecured name," as recited in claim 1.”

3PR presents that “Second, the Patent Owner argues Lendenmann does not disclose a device that has both a "secure name" and an "unsecure name." Specifically, while Patent Owner acknowledges that Lendenmann refers to both X.500 and DNS as naming schemes, it asserts there is no "nexus between X.500 names and secure communications" shown in Lendenmann. Second Response at 17. The Office has already rejected this argument, finding that "X.500 satisfies the requirement for a secure name, as the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address." ACP at 58. The Office also explained that the X.500 naming scheme of the DCE environment "is a secure, internal naming convention." ACP at 58 (citing Request at 105). For example, the Request explained that resolution of the X.500 names is controlled by the CDS, which is integrated into the security server of the X.500 system and will only complete an operation "if the user is authenticated and authorized." Request at 104. Thus, as explained in the ACP and the Request, DCE cells, as well as the objects within them, can have both an X.500 name (a "secure" name) and a DNS name (an "unsecure" name), and the Office correctly found that Lendenmann discloses "a first device associated with a secure name and an unsecured name." ”

The Examiner agrees with the 3PR, as device aliasing is discussed in Lendenmann where an alternate name is used to refer to a device in addition to its traditional DNS name. Here the "cell has a primary name, which is the name that DCE services return for the cell when queried, and one or more alias names that the DCE service recognize in addition to the primary name. For example, if your cell is registered in the GDS global directory service, and you want to register it in the DNS as well, you obtain a DNS name for the cell, and set it up as a cell alias.” (see page 24).

Here X.500 satisfies the requirement for a secure name, as the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address. Conversely, the if an Internet Address alone is used then a traditional DNS is used to access, leaving the address unsecured and out in the open.

The system of Lendenmann allows users to access by name resources such as server, files, disks, etc. without using the network address (though it has one), but rather using an alternate naming scheme (see page 22, first paragraph).

(ii)

PO argues “The Office is incorrect because Lendenmann does not disclose hiding Internet addresses or accessing Internet addresses outside of the DCE directory service.

First, Lendenmann does not disclose hiding Internet addresses. Rather, as the Office clearly states in another section of the Second Office Action, the CDS has a simple function in a client/server context: "when given a name, CDS returns the network address of the named resource." (Id. at 56, citing Lendenmann 21, emphasis added.) This happens regardless of whether an X.500 name or a DNS name is used, since the directory service supports both "for interoperability purposes." (Lendenmann 21.) Because the Office's rationale for concluding that an X.500 name corresponds to a "secure name" is contrary to the teachings of Lendenmann, the rejection should be withdrawn.

Second, Lendenmann does not disclose accessing Internet addresses outside of the DCE directory service. Rather, Lendenmann explains that both DNS and X.500 names are used within the DCE directory service: "There are two well-established schemes in place that DCE makes use of: CCITT X.500 [and] Internet Domain Name

Service (DNS)." (Id. at 23.) The Office again provides no citation or support for its assertion that if a DNS name were used, a "traditional DNS [would be] used to access, leaving the address unsecured and out in the open." (See Second OA at 58.) Rather, Lendenmann utilizes both X.500 and DNS names within its DCE, and the Security Service performs its authentication and authorization features regardless of whether an X.500 or DNS name is used. (Lendenmann 34.)”

3PR presents that “Third, Patent Owner argues that Lendenmman does not disclose "secure" names because it does not "hid[e] Intemet addresses" and does not disclose accessing Internet addresses outside of the DCE environment. Patent Owner's arguments can be dismissed based on the Office's construction of the term "secure name" and the actual teachings of Lendenmann. A name may be found to be secure if it is stored in a secure location and whether it can be resolved by a conventional name server. X.500 names satisfy this definition. As Lendenmann explains, addresses in its system are hidden because queries to the CDS, which is integrated into the security server, are made within the confines of the DCE cell and can also be encrypted. ACP at 58-59. Further, whether the Lendenmann systems access Internet addresses outside of the DCE environment has no relevance to the question whether Lendenmann discloses a device having a "secure name" and an "unsecure name." Lendenmann presents the X.500 scheme, which is "a secure, internal naming convention," and the DNS scheme, which is a naming convention based on the public Internet DNS system is unsecure (e.g., because conventional name servers are publicly accessible and resolve conventional domain names in a manner that provides no inherent security). Because

Patent Owner's arguments are all based on improper claim constructions and a misunderstanding of the Lendenmann systems, the Office should disregard them and maintain the rejection of claim 1 as anticipated by Lendenmann."

The Examiner agrees with the 3PR, as whether the systems access Internet addresses outside of the DCE environment or not this doesn't preclude the use of Lendenmann, as Lendenmann is shown to provide the X.500 naming scheme as in internal secure alternate naming scheme that supplements the traditional naming scheme.

b. First device

PO argues "the Office relies on a DCE cell as the "first device" for some features of claim 1, while relying on a specific server for other features of a "first device." Accordingly, the rejection of claim 1 should be withdrawn because the Office has failed to show how Lendenmann discloses "all of the limitations arranged or combined in the same way as recited in the claim." NetMoneyIN, Inc. v. VeriSign, Inc., 545 F.3d 1359, 1371 (Fed. Cir. 2008)."

…

"The "first device" is again recited in the claim 1 feature of "receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desire[] to securely communicate with the first device" (emphases added). For this feature of claim 1, the Office changes its position and relies not on a DCE cell as corresponding to the "first device," but rather a particular Lendenmann server. (Second OA at 59, citing Req. at 106-08.)"

3PR presents that "What the cited portions of the ACP and the Request explain is that either the DCE cell or the RPC server may be a "first device" due to the broad language used in claim 1. For example, Lendenmann shows that during the RPC binding process, an RPC client uses the name service interface (NSI) to make a request to the appropriate CDS server to get an address associated with a compatible RPC server, which can be identified by a DNS address or an X.500 address. Request at 106-07. The RPC client then sends a request to establish a communications channel to the RPC server in which it can request that security protocols be implemented. Request at 107-08. Future communications between the RPC client and server are then secure. The first device thus can be either the RPC server or, if the client and server are in different DCE cells, the DCE cell to which the RPC server belongs. Because the RPC server is a part of that DCE cell, any communications sent to or from the RPC server will necessarily be sent to or from the DCE cell. Consequently, any "secure name" associated with the RPC server necessarily is also associated with the DCE cell, so the Office's rejection was proper and should be maintained."

The Examiner agrees with the 3PR, that both the DCE cell and the RPC server may be interpreted as a "first device".

2.

a.

PO argues “Requester did not contradict or contest Patent Owner's detailed arguments regarding the RPC binding process. (Comments at 22-23.) Neither did the Office. (Second OA at 61-63.) Instead, Requester and the Office now rely on a non-RPC feature of Lendenmann as allegedly showing the "sending a message to a secure name service" and "receiving a message" features of claim 2, rather than the RPC binding process. (Comments at 22; Second OA at 62-63, citing Lendenmann 21.) This revised argument, now relying on multiple embodiments for various features of claim 2, fails to support the rejection.”

3PR presents that “The basis of the Office's rejection of claim 2 has not changed between the First Action and the ACP. In both, the Office and the Requester have relied on the same process, the RPC binding process, to show how the limitations of claim 2 are met. Request at 109-15; First Action at 12-13; ACP at 61-64. For example, in explaining how the elements of claim 2 were satisfied, the Office described a portion of that process--querying the CDS for a network address--that used a client server model. Patent Owner contends this is a new rejection by incorrectly asserting that it combines elements of the client server and RPC models. In reality, the querying process is part of the RPC binding process, as was explained in the Request and the First Action. "The CDS is a secure name service," and it controls access to "' [n]ames in the namespace, including clearinghouses, directories, object entries, softlinks, and child pointers.'" Request at 112-13 (quoting Lendenmann at 34). The Request also explained that RPC applications can post and access information on the CDS using the Name Service

Interface (NSI): "'Using the NSI export operation, an RPC server can place information about its interfaces, objects and addresses into a namespace entry. Using NSI import operations, the RPC clients can access this information.'" Request at 107 (quoting Lendenmann at 178-79). The Office also observed in the First Action that this information is used during the RPC binding process, "[w]here the client can utilize the namespace maintained by the CDS for the location of a server that handles the interface that the client is interested in." First Action at 12 (citing Lendenmann at 182). Simply put, there is nothing new about the Office's analysis, nor does it rely on a "disjointed" combination of components that are described in Lendenmann."

The Examiner agrees with the 3PR, as the further specification of the interoperability of the querying process and the RPC binding provided in the last action was provided to further ground the rejection, while not changing the grounds of the rejection, and was provided responsive the Patent Owner's contentions.

PO argues "the Office argues that with regard to "picking and choosing" arguments, "if these are all features available in Lendenmann, and if a combination of the features described in Lendenmann are usable together, then it properly rejects the claims." (Second OA at 63.)"

3PR presents the way the combination of features are described as used together, as presented above.

The Examiner agrees with the 3PR regarding how Lendenmann describes and clearly lays out how the different models are usable together to implement the secure network data transmission in the Distributed computing environment.

b. “Secure Name”

PO argues “As discussed above in Section V.A.I.a.i, the Office and Requester incorrectly interpret "secure name" in a manner that is inconsistent with the specification. This interpretation, relying on out-of-context external statements, reads the term "secure" out of the plain claim language and fails to comport with the portions of the specification on which those external statements rely. Moreover, because Lendenmann merely discloses that X.500 and DNS names are alternatives to each other for cell-name aliasing, and because Lendenmann provides a separate security service that operates the same regardless of whether X.500 or DNS names are used, the X.500 and DNS names are neither secure nor unsecured, as explained in Patent Owner's previous Response. (See Response at 33-36.)”

3PR presents that “As explained above in the discussion of the basis of the rejection of claim 1, Patent Owner's arguments rest on its belief the claims incorporate limitations shown for specific examples in the specification. The claims do not, as explained above. Moreover, Patent Owner's assertions are inconsistent with its prior representations to the Office as to what a "secure name" may constitute.”

The Examiner agrees with the 3PR, as the Patent Owner has further submitted in Applicant Remarks/Arguments at 9 (Oct. 8, 2010):

> *"[T]he Applicant submits that a "secure name" is a name associated with a network address associated of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device.* ***The claimed "secure name" includes, but is not limited to, a secure domain name. For example, a "secure name" can be a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scom) or a telephone number."***

Where the X.500 address is an alternate address that is used in place of the actual IP address and resolved by an intermediate directory server, much like that described in the '181 Patent.

C. "Second Device"

PO argues "The Office incorrectly mixes and matches features of Lendenmann as corresponding to the "second device" of claim 2 for different features of the claim. For instance, the Office identifies only a DCE cell as potentially having an X.500 name--the alleged "secure name" in claim 2. (Req. at 111, relying on Lendenmann 23, discussing "Cell Names.") A DCE cell is defined as "a group of users, systems and resources that are typically centered around a common purpose." (Lendenmann 20.)

Lendenmann further explains that "[e]ach cell is a self-sufficient, independently managed unit in a global distributed computing environment" that contains at least one Security Server, one CDS, and three DTS Servers per LAN. (Id. at 21 .) But for the features of sending and receiving "a message" in other portions of claim 2, the Office relies on a particular server (not a DCE cell) as corresponding to the claimed "second device." (Req. at 112-15, citing Fig. 68, reproduced above in Section V.A.l.b.) So again, the Office has not shown how Lendenmann discloses "all of the limitations arranged or combined in the same way as recited in the claim." Net MoneyIN, 545 F.3d at 1371; Therasense, 593 F.3d at 1332."

3PR presents that "As explained above with respect to claim 1, a "first device" can be either the RPC server or, if the client and server are in different DCE cells, the DCE cell to which the RPC server belongs. Similarly, a "second device" can be either the RPC client or, if the client and server are in different DCE cells, the DCE cell to which the RPC client belongs."

The Examiner agrees with the 3PR, as the client / server communication being treated as the two ends of the secure translation of data is clear from the record.

D. "Secure Name Service"

PO argues "Requester's claim interpretation contradicts the embodiments in the patent specification on which the statements from the ' 180 patent reexamination are based. (See Order at 5, citing ' 180 patent 51:25-35, corresponding to ' 181 patent

50:15-25.) In this embodiment of the ' 181 patent specification, when the standard top-level domain name is replaced with the secure top-level domain name, "software module 3309 sends a query to SDNS 3313." ('181 patent 50:36-39, describing step 3408 of Fig. 34.) Then, in step 3409, "SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link." (Id. at 51:15-17.) Thus, the SDNS embodiment on which Requester's claim interpretation is ultimately based in fact actively coordinates with the VPN gatekeeper to establish a VPN communication link, and therefore "further support[s] establishing a secure communication link," as discussed in Patent Owner's previous Response. (Response at 36- 37.) Requester's selective reliance on out-of-context external statements is incorrect, inconsistent with the specification, and insufficient to support the rejection."

3PR presents that "There also is no "contradiction" between the Office's definition of "secure name service" and the ' 181 specification, as Patent Owner contends. Second Request at 23. The example Patent Owner cites from the specification falls within the scope of the Office's construction of "secure name service." Patent Owner's new opinions about the scope of this claim term is, thus, not a "contradiction" but simply a difference of opinion with the Office. If Patent Owner wishes the terms of its claims to have a different scope than what is compelled by the plain language used in those claims, it must amend the claims to correspond to that desired meaning. Because it has not done so, the Office must disregard Patent Owner's arguments that Lendenmann does not disclose a "secure name service.""

The Examiner agrees with the 3PR, as there is no way that "software module 3309 sends a query to SDNS 3313" and "SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link", can be read into the claim by simply claiming a "Secure Name Service". Under the broadest reasonable interpretation of the claims language Lendenmann's Directory Servers provide software means for linking secure (non-location bearing names) to actual IP addresses.

PO argues "The Office provides no support from Lendenmann for its assertion that the CDS/GDS does something different when it is provided a DNS name, compared to when it is provided an X.500 name."

3PR presents that "he capacity of the Lendenmann systems to act on X.500 names shows that those systems are a "secure name service" within the meaning of the claims. The claims require nothing more. Moreover, there is no requirement in the claims that a system that can function as a "secure name service" cannot also function as an "unsecure" name service. The contrast Patent Owner tries to make can simply be disregarded as it is irrelevant to what has been claimed."

The Examiner agrees with the 3PR, as support was provided in the Lendenmann reference only for what has been claimed, where Lendenmann teaches a name that hides the address and is later mapped to still reach its destination.

e. “Sending a Message to the Network Address Associated with the Secure Name of the Second Device Using a Secure Communication Link”

PO argues “Requester did not substantively address Patent Owner's arguments. Requester complains that Patent Owner "employs a fundamentally implausible reading of Lendenmann" by arguing that no nexus exists between RPC security features and X.500 names, (Comments at 23), but provides no basis in Lendenmann nor any declarations or other support for its arguments, e.g., such as to try to allegedly show that Lendenmann differentiates between its use of X.500 names and DNS names. (But see Lendenmann 21, explaining equivalent use of DNS and X.500 "for interoperability purposes.") Thus, Requester's arguments were nothing more than irrelevant attorney argument, and fail to support the rejection to the extent relied upon by the Office. (Second OA at 64.)”

…

“the Office cites Lendenmann for the proposition that an RPC client can choose a level of protection for authenticated RPC. (Id.) The Office appears to contend that the allegedly resulting authenticated RPC corresponds to the "secure communication link" of claim 2. (Id., quoting Lendenmann 192.) Yet even if one were to incorrectly assume that the Office has shown a "secure communication link," the Office has not demonstrated that Lendenmann discloses the rest of the claim features of "sending a message to the network address associated with the secure name of the second device using a secure communication link" (emphasis added). On these features, the Second Office Action is silent despite Patent Owner's detailed arguments traversing the rejection.""

3PR presents that "The Office correctly found that Lendenmann discloses sending a message to the network address associated with a secure name of the second device using a secure communication link. In its Second Response, Patent Owner simply repeats argument it presented in its First Response that no "nexus" exists between security and X.500 names. In the ACP, the Office properly rejected this argument, and it can do so again without further comment. As the Office and the Request each explained, the X.500 name service shown in Lendenmann is inherently a secure function because it only is available within a secure network environment. Request at 103-05; ACP at 56, 58. In addition, the claims impose no specific type of connection between the secure name service and the overall functioning of the claimed systems."

The Examiner agrees with the 3PR, as the X.500 satisfies the requirement for a secure name, as the address must be resolved through the directory service component, where the name is provided for the destination, thereby hiding the actual address. Conversely, if an Internet Address alone is used then a traditional DNS is used to access, leaving the address unsecured and out in the open. As the Patent Owner admitted in the last response: The Security Service thus weeds out unauthorized users without regard to the naming scheme employed by each user (X.500 or DNS).

(Lendenmann 34; Keromytis Decl. ¶ 63.), Where Lendenmann provides the further level of security by using the alternate naming scheme.

PO argues "The Office also did not substantively address Patent Owner's arguments".

3PR presents that "Patent Owner also complains that the Office failed to address its prior arguments. This is incorrect; Patent Owner is simply unhappy that the Office found those arguments unpersuasive and did not adopt them. The Office was correct in doing so. For example, in its First Response, Patent Owner sought to read unclaimed limitations from the specification into the claims to prohibit the implementation of any security measures when an "unsecure name" was used. First Response at 39-40. The Office correctly found that the claims imposed no such limitation, and concluded that Lendenmann discloses exactly what the claims require: "sending a message to the network address associated with the secure name of the second device using a secure communication link." Patent Owner's attempts to read limitations from the specification into the claims should again be rejected, and the rejection of claim 2 should be maintained."

The Examiner agrees with the 3PR, as a clear mapping and detailed discussion has been provided in the Action Closing Prosecution as to how Lendenmann reads upon the disclosed claim phraseology.

3. Dependent Claims 5 and 6

PO argues “The Office has not identified any encrypted messages containing network addresses in Lendenmann, and Lendenmann in fact discloses none. (Id.) Thus, the maintained rejection should be withdrawn for the reasons in Patent Owner's previous Response. (Response at 40-41 .)

Meanwhile, Requester's arguments regarding RPC procedures are irrelevant because, as discussed above in Section V.A.2.a, the RPC communication model of Lendenmann does not involve requesting or returning network addresses associated with any particular secure name. (Comments at 24; Response at 40-41.) Rather, within RPC, a CDS identifies servers to the client based on functional criteria other than server names. (See supra Section V.A.2.a, Response at 37-38.)”

3PR presents that “the CDS is part of Lendemann's security service and the security service provides for encrypted communication between devices. ACP at 65. Thus, Lendenmann discloses "receiving the message containing the network address associated with the secure name of the second device.., in encrypted form" and "decrypting" that message.”

The Examiner agrees with the 3PR, as was pointed out on page 65 of the ACP - “the use of RPC routines in order to query the CDS. Request at 117-119. Further, as already demonstrated above, clients can establish a level of protection with an established RPC that "determines the degree to which client server messages are actually encrypted." Request at 119." So in communication between devices utilizing the Directory server the messages are shown to be encrypted to transmission.

4. Dependent Claim 21

Patent Owner's argues only for reasons previously discussed, and therefore is directed to the above responses by the 3PR and the Examiner and the Action Closing Prosecution.

5. Independent Claim 24 and Dependent Claim 25

Patent Owner's argues only for “reasons set forth above”, and therefore is directed to the above responses by the 3PR and the Examiner.

PO argues “a non-final office action is in order because the issues in this proceeding, including what the Office means by "secure" and "unsecured," remain far from settled. M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed.").”

3PR presents that “There is nothing unsettled about the claim construction the Office has employed - it has remained constant throughout this proceeding. This comment is simply another transparent attempt by Patent Owner to improperly delay these proceedings.”

The Examiner agrees with the 3PR, as the Offices interpretation of "secure" and "unsecured" has remained consistent through the reexamination. The contention by the Patent Owner providing differing interpretation of how the claim should be limited by those terms is not convincing so as to reopening prosecution.

6. Independent Claim 26 and Dependent Claim 27

PO argues “Lendenmann does not disclose that an X.500 name has its own unique corresponding network address.”

3PR presents that “Lendenmann also shows that each device has a unique network address, and that the X.500 name is associated with that address. As the Office explained in the ACP, "The X.500 and domain names associated with a device in the Lendenmann scheme thus comprise both a unsecure and a unique secure network address .... [T]he whole purpose of addressing is for the locating of unique network locations, where Lendenmann teaches means for providing naming to network ends where the name corresponds to a specific network address." ACP at 68-69.”

The Examiner agrees with the 3PR, as for the reasons set for in the ACP and as described above. The X.500 name is directly mapped to a unique corresponding network address through the directory service (further see page 10).

PO argues “the Office changes its argument in the Second Office Action to now assert that an X.500 name itself is the recited "unique network address." (Second OA at 68, "The X.500 and domain names associated with a device in a Lendenmann scheme thus comprise both a[n] unsecure and a unique secret[] network address," emphasis added; compare Req. at 142.)"

…

"the Office's rejection is based on an alleged embodiment in which only two of the three recited claim features ("secure name," "unsecured name," and "unique network address correspond[ing] to the secure name") could possibly be present."

3PR presents that "Here, the claims require registration of an "unsecured name associated with the first device" and "registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name." A device in the Lendenmann scheme can be registered with the CDS to be associated with a domain name and also with an X.500 name. This is all that the claims require (i. e., registration with a unsecure and with a secure name)."

…

"As the Office explained in the ACP, "The X.500 and domain names associated with a device in the Lendenmann scheme thus comprise both a unsecure and a unique secure network address .... IT]he whole purpose of addressing is for the locating of unique network locations, where Lendenmann teaches means for providing naming to network ends where the name corresponds to a specific network address." ACP at 68-69. The Office correctly found that Lendenmann discloses all the limitations of claims 26 and 27."

The Examiner agrees with the 3PR, as Lendenmann presents a name which hides the destination (X.500), a name which provides destination in an unsecure manner (domain name), where the user can use the provided name to access the unique network address (Internet Address) utilizing the Domain Name Service (further see page 10).

7. Independent Claims 28 and 29

Patent Owner's argues only for “reasons similar to those described above”, and therefore is directed to the above responses by the 3PR and the Examiner.

8. Dependent Claims 3-9, 12-15, and 18-23

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

B. (ISSUE 7)

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

C. (ISSUE 8)

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

VI. The Rejection of Claims 1-23 and 28-29 under Provino (ISSUE 9)

Overview

Provino teaches use of an unsecured name where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43). Provino further teaches use of a secure name (domain name or other human-readable Internet address) where the device my only establish a secure communication link upon receipt of the secure name (see column 9, line 56 through column 10, line 7, column 9, lines 17-27, and column 13, lines 26-67), Provino teaches that "*the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30.*" (see column 13, lines 54-67) Here the initiating device has the email address / domain name and requests the actual IP address. Furthermore, encrypted data transmission is utilized in Provino where encrypted messages are sent with a decryption key for eventual decryptions (see column 9, line 56 through column 10, line 7).

A.

PO argues "the Office adopted a new rejection related to Provino, shifting the focus from a domain name to an Internet address. The Request originally alleged that two different domain names in Provino are the claimed "secure name" and "unsecured name""

3PR presents that “the manner in which the Request, the First Office Action and the ACP each refer to the disclosure of a "secure name" in Provino has remained consistent. For example, the Request, which was incorporated into both the First Office Action and the ACP, explained:

> Provino explains that these DNS systems include secure nameservers (e.g., Nameserver 32 in Figure 1) that "serves to resolve human-readable Internet addresses for servers 31 (s) internal to the virtual private network 15 to respective integer Internet addresses.

Request at 170 (citing Provino at 8:67-9:5). Patent Owner ignored this observation in its First Response. This passage shows that a domain name acted on by Nameserver 32 (and which is resolvable into an IP address, i.e., an "integer Internet address") comprises a "secure name" as specified in the ' 181 patent claims. Thus, the Office has not changed its position on what Provino teaches, much less changed the statutory or substantive basis of the rejections.”

The Examiner agrees with the 3PR, as the office has consistently maintained that the secure name server "serves to resolve human-readable Internet addresses for servers 31 (s) internal to the virtual private network 15 to respective integer Internet addresses. Again this maps well to the claims which require an alternate name (such as this human-readable name, which is resolved through the name server to provide the Internet address.

B. Independent Claim 1

1. “First Device” and “Second Device"

PO argues “Requester mixed and matched features from two different devices in its attempt to show unpatentability. (See Response at 47, quoting inconsistencies in the Request.) Requester now contends that a server 3 l(S) is the claimed "first device" and a device 12(m) is the claimed "second device." (Comments at 26-28.) The Office does not identify which device is first and which is second, (see Second OA at 74), but based on the Office's apparent agreement with Requester, Patent Owner assumes that the Office is also treating server 31(S) as the claimed "first device" and device 12(m) as the claimed "second device".

3PR presents that “The criticisms levied by Patent Owner are unfounded - Requester's position is unchanged. For example, the Request and First Office Action both pointed out that server 31 (S) is the claimed "first device" and "device 12(m)" is the claimed second device in Provino. See, e.g., Request at 168-71; First Action at 15-17. Patent Owner's criticisms are simply baseless.”

The Examiner agrees with the 3PR, as the position of the office and the 3PR have not changed and it appears we are all in agreement as to what the position is.

2. "a Network Address Corresponding to the Secure Name Associated with the First Device"

PO argues “The Office now contends that the claimed "secure name" is "the integer Internet address which is registered on the VPN name server." (Id. at 71.) However, if this address is the claimed "secure name," it is not clear what the Office contends is the claimed "network address corresponding to the secure name." It appears that the Office is relying on the "integer Internet address which is registered on the VPN name server" as being both the "secure name" and the "network address corresponding to the secure name." The claims and specification, however, differentiate between those two terms, and the same "integer Internet address" cannot qualify as both. To contend otherwise effectively reads "receiving, at a network address corresponding to the secure name" out of the claim, as the Office's interpretation reduces that clause to either "receiving, at the secure name" or "receiving, at a network address," since the Office apparently equates the secure name and the network address. This is not a reasonable interpretation of the claim, which expressly requires both a "secure name" and "a network address corresponding to the secure name.""

3PR presents that "As noted above, the Office has consistently explained that the domain names in nameserver 32 of Provino constitute the "secure name(s)" disclosed in the '181 patent claims. Thus, as explained in the Request (at 174-175, for example) and the ACP (at 71- 73), the "integer Intemet address," which is resolvable from the domain name, is the "network address corresponding to the secure name associated with the first device." Patent Owner also contends reading Provino in this manner "effectively reads" clauses out of the claims"

The Examiner agrees with the 3PR, as Provino teaches use of an **unsecured name** where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43). Provino further teaches use of a **secure name** (domain name or other human-readable Internet address) where the device my only establish a secure communication link upon receipt of the secure name (see column 9, line 56 through column 10, line 7, column 9, lines 17-27, and column 13, lines 26-67), Provino teaches that "*the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the* ***integer Internet address*** *associated with the human-readable Internet address."* (see column 13, lines 54-67) Here the initiating device has the email address / domain name and requests the actual IP address.

3. "Unsecured Name"

PO argues "The Office contends that "Provino teaches the use of an unsecured name where access is provided through a public domain name server (see column 1, lines 56-60 and column 8, lines 40-43)." (Id. at 69; see also id. at 71.) Provino, however, teaches that public domain name server 17 does not contain any names or addresses associated with server 3 I(S). It states that "nameserver 17 is not provided with integer Internet addresses for servers 31 (S) and other devices which are in the virtual private network 15." (Provino 10:48-51, emphasis added.) Thus, "the device 12(m), after the operator has entered the human- readable Internet address, will not be able to obtain the integer Internet address of the server 31 (S) which is to be accessed from that nameserver 17." (Id. at 10:52-55, emphasis added.)"

3PR presents that "First, the claims do not restrict a "device" to a single component shown in the Provino systems considered in isolation. Instead, as explained in the Request and the prior actions from the Office, the Provino devices comprise multiple components that interact with each other to provide the functionality specified by the claims. Request at 167-72; First Action at 15-17; ACP at 69-74. Thus, the claims do not require one component in Provino to perform all the functions specified in the claim. Second, in the ' 181 disclosure, Patent Owner identifies multiple discrete components that interact with each other to provide specified functionalities. See, e.g., Fig. 26 showing DNS server 2609 and DNS Proxy 2610 interacting with "Gate Keeper" 2603 to handle and resolve secure vs. unsecure names. The Office, thus, correctly refuted Patent Owner's incorrect contentions about the capacities and functions of the Provino system. See ACP at 71- 72."

The Examiner agrees with the 3PR, and further adds that the claim only requires "a first device associated with a secure name and an unsecured name", where just because a human-readable domain name is used to access the node, doesn't relieve it from the fact that it is accessible traditionally via the "n"-bit integer address it has natively (see column 1, lines 36-61).

4. Firewall-Based System

PO argues "Placing a conventional domain name server behind a firewall does not convert it from being conventional into a secure domain name server. As the '181 patent specification explains, a secure domain name server must possess additional functionality not present in a conventional domain name server, and it specifically distinguishes the invention from the functions of a conventional domain name server.

(See Response at 45-46, explaining how the patent specification disparages systems like Provino's and how the claims cannot be read to encompass those systems.) Without a secure domain name server, Provino cannot disclose secure names. Therefore, it does not disclose, teach, or suggest at least the claimed "first device associated with a secure name and an unsecured name," and "receiving, at a network address corresponding to the secure name associated with the first device.""

3PR presents that "Provino shows a system comprising multiple components that work together to receive, at a network address corresponding to a secure name associated with a destination device (e.g., firewall 30, VPN name server 32) a message from a second device to securely communicate. See, e.g., Provino at Fig. 1. The routing of a request to that destination where it is evaluated and acted upon is part of the Provino system, which means the message will also be received, inter alia, by device 12(m) and Name Server 17. If the request specifies a desire to "securely communicate" (e.g., by requesting access to a secure resource within VPN 15 in Provino), and the user's credentials are valid, then a VPN is established, and a message (e.g., data for the requested resource) is sent to the requesting entity (the "second device" in claim 1). Moreover, explained in the Request and ACP, the VPN Server 32 is not accessible in the same manner as a conventional domain server. Instead, the Provino VPN Server 32 facilitates a secure communication link with authorized devices in the same manner as the "secure name service" described in the ' 181 patent."

…

“Second, the unspecified "additional functionality" Patent Owner refers to is neither identified by it nor is it actually claimed. Instead, the claims by their literal terms encompass the exact systems described in Provino. Requester again observes that Patent Owner's "disparagement" theory is factually incorrect and legally irrelevant in this proceeding. For example, the original prosecution history does not show that Patent Owner "disparaged" secure domain name servers such as those shown in Provino. In fact, the secure name servers in the ' 181 specification mirror precisely the Provino scheme.”

The Examiner agrees with the 3PR, as the additional special functionally and elements that supposedly differentiate it from the Provino system are simply not claimed.

C. Independent Claim 2

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

D. Dependent Claims 3-15 and 18-22

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

E. Dependent Claim 23

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

F. Independent Claim 28

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

G. Independent Claim 29

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

VII. Rejections over Provion and H.323 (ISSUE 10)

PO argues “the Office revised its interpretation of the applicability of Provino to the rejected claims and issued a new rejection based on that new interpretation. The Office is presumably applying that new interpretation to its obviousness rejection for claims 24-26, but it has provided no explanation of the alleged interplay between that new interpretation and the alleged teachings ofH.323. There is no explanation in the Second Office Action of how or why one of ordinary skill in the art would have combined H.323 with Provino under the Office's new interpretation.”

3PR presents that “the basis for the rejection was clearly explained in the Request and the First Action, and has not changed in the ACP. See Request at 188-201; First Action at 18; ACP at 75. Patent Owner's assertion that the Office has changed its interpretation of Provino and the rejected claims, thus, is incorrect. See §H above Provino."

The Examiner agrees with the 3PR, as explained above, the grounds of the rejection have not been changed, therefor the original reasons for combination still apply.

PO argues "The Office appears to continue to rely on the teachings ofH.235 as though they are part of H.323. (Id. at 75-76.) But simply referencing another document is not sufficient to incorporate that document by reference. See Advanced Display Sys., Inc. v. Kent State Univ., 212 F.3d 1272, 1282 (Fed. Cir. 2000)."

3PR presents that "the Office properly rejected Patent Owner's "improper incorporation by reference" theory regarding the teachings ofH.323 and H.235. See ACP at 75-76. As the Office pointed out, H. 323 expressly incorporates H.235 as "constituting provisions of this [i.e., the H. 323] Recommendation" (see Request at 204 (citing H. 323 at 2-3)) and by stating that "[A]uthentication and security.., if it is provided, it shall be provided in accordance with Recommendation H.235, Request at 206 (citing H.323 at 81) (emphasis added). See also ACP at 76 ("The Examiner agrees with the third party Requester, H235 is being reference as a standard for security and encryption of H-Series multimedia terminals")."

The Examiner agrees with the 3PR, as H235 is being referenced as a standard for security and encryption of H-Series multimedia terminals, specifically noting H.323, where the further features pointed out of H.235 are merely features of the standard.

PO argues “While it is not clear how the Office contends the claims are obvious over Provino in combination with H.323 by itself or also in combination with H.235, Patent Owner is not aware of any reasonable interpretation of those references that teaches all of the claimed features of claims 24-26.”

3PR presents that “The basis for the rejection of these claims 24-26 is clearly explained in the Request, the First Action and the ACP. Request at 188-201; First Action at 18; ACP at 75. As Patent Owner presents no response specific to the combination of Provino with H. 323, there is no basis for the Office to withdraw its previously imposed rejections, which should be maintained.”

The Examiner agrees with the 3PR, as the rejection has been provided with specific reference to the references pointed out for each claim limitation.

VII. The Rejection of Claims 1-29 under H.323 (ISSUE 11)

A.

PO argues “H.323 does not state that allprovisions of the listed references are part of H.323--it states only that those references contain provisions that are part of H.323 when referenced in the text. Despite the explicit limitations in this statement, the Office nevertheless asserts that it suffices to incorporate the listed documents in their entireties. (Id.)”

3PR presents that “as explained in the Request, H.323 expressly incorporates H.245, H.235, and H.245 as "constituting provisions of this [i.e., the H.323] Recommendation." Request at 204 (citing H.323 at 2-3). That is sufficient to incorporate the teachings ofH.245, H.235, and H.225 in their entirety. See Harari v. Lee, 656 F.3d 1331, 1335 (Fed. Cir. 2011) (holding "broad and unequivocal" language sufficient to incorporate the entire disclosure of another reference). Even under stricter standard proposed by Patent Owner, each ofH.245, H.235, and H.245 was properly incorporated by reference. For example, H.323 explains that "authentication and security for H.323 is optional; however, if it is provided, it shall be provided in accordance with Recommendation H.235." Request at 204-05 (citing H.323 at 81 (emphasis added)). Similarly, H. 323 discloses that products claiming compliance with Version 2 of H.323 shall comply with all of the mandatory_ requirements of H.323 (1998) which references Recommendations H.225[] (1998) and H.245 (1998)." Request at 205 (citing H.323 at (i) (emphasis added)). H.323 also describes H.225 as containing "[c]all signaling protocols and media stream packetization for packet based multimedia communication systems," and H.245 as containing "[c]ontrol protocol for multimedia communication." Request at 206-08 (citing H.323 at 2-3). Each of these statements was identified in the Request, the First Office Action, Requester's comments, and the ACP. Patent Owner continues to ignore these statements in its latest response. Because H. 323 incorporates by reference the teachings of H.225, H.235, and H.245, the Office's rejection was proper and should be maintained.”

The Examiner agrees with the 3PR, each of the documents, even if only incorporated for a relevant portion of their entire disclosure, would still incorporate the portions relied upon in the rejection. However, the office still believes that specific incorporating langue was provided in the H.323 to incorporate the entire disclosure as the separate portion of the standard(s) are clearly usable together.

B.

PO argues “Even if one were to incorrectly assume that all of the asserted references are incorporated by reference into H. 323, this does not give the Office license to selectively pick and choose from among multiple embodiments in these various documents to allege disclosure of each of the different, particular elements recited in the '181 patent claims. Net MoneyIN, 545 F.3d at 1371 (quoting 455 F.2d at 587).”

3PR presents that “These belated comments should be disregarded as they are not timely. In addition, they should be rejected because Patent Owner does not identify any specific features of H. 323 that were improperly combined. Were the Office to even consider Patent Owner's vague objection, it would be left to guess at which features Patent Owner believes were improperly combined. Finally, Patent Owner's assertions are premised on the mistaken belief that the IPsec protocol cannot be used when an endpoint is protected by a security token. Indeed, H.323 clearly shows that IPsec is used with security tokens and that IPsec and tokens are part of the same embodiment.

Request at 218-26. Because the Office correctly found that H.323 incorporates the teachings of H.225, H.235, and H.245, the rejection of the claims over H. 323 were proper and should be maintained."

The Examiner agrees with the 3PR, as specific cases of "mixing and matching" have not been pointed out.

1. Independent Claim 1

PO argues "Rather than maintain its prior arguments for the rejection, the Office instead proposed a new one: that a "name and address . . . linked via a registry" correspond to the secure name and unsecured name recited in claim 1. (Second OA at 80.) The Office explains that the alleged secure name is a "generic name . . . such as a phone number or email address," while "the address itself (capable of accessing the network end), is an unsecure means of access." (Id.) The Office's new rejection is incorrect and should be withdrawn."

…

"the Office is incorrect that a "generic name . . . such as a phone number or email address" corresponds to the "secure name" recited in claim 1. The Office offers no support for its assertion, (see Second OA at 80), and claim 1 recites a "secure name," not a "generic name," so the new rejection has no bearing on the claim language."

3PR presents that "Patent Owner misunderstands the H.323 disclosure and the ACP. The ACP did not set forth a new basis for the rejection - the passage referenced by Patent Owner merely refers to a different part of the process described in H.323 that was identified in the Request and the First Action. Specifically, the Request and the ACP explain that H.323 discloses that each device in an H.323 network "is associated with one or more alias names, called Alias addresses, which can be in the form of a phone number or an email address." ACP at 79 (quoting Request at 204). Alias addresses are "secure," in part, because they are "protected by 'access tokens,' which have the function of ensuring the anonymity of an endpoint's Transport and Alias Addresses." ACP at 79 (quoting Request at 204). The Request also explained that a device will "be[] associated with the unsecured names of the Gatekeeper computer with which they are registered," (Request at 210), and will also "register[] an Access Token instead of a regular Alias address with the Gatekeeper to secure its name and to receive communications at the network address associated with the secure name," (Request at 213)."

The Examiner agrees with the 3PR, as these alias address are said ensure anonymity, by not revealing the actual address of the component.

PO argues "The Office is also incorrect that an address "capable of accessing the network end" (i.e., a network address) corresponds to an "unsecured name." (See Second OA at 80.) Claim 1 recites two separate names--a "secure name" and an "unsecured name"--as well as "a network address corresponding to the secure name." The Office attempts to conflate the "unsecured name" and "network address" claim terms. As a result, the Office's rejection is based upon an arrangement of H.323

features in which only two of the three recited claim features ("secure name," "unsecured name," and "network address corresponding to the secure name") could possibly be present."

3PR presents that "The Request also explained that a device will "be[] associated with the unsecured names of the Gatekeeper computer with which they are registered," (Request at 210), and will also "register[] an Access Token instead of a regular Alias address with the Gatekeeper to secure its name and to receive communications at the network address associated with the secure name," (Request at 213)."

The Examiner agrees with the 3PR, as the alias is specially tied to a network address.

b.

PO argues "he Office's arguments do not account for the specific recitations in claim 1, i.e., that the alleged "message" of claim 1--the Office's "request to communicate"--is modified by the phrase "of the desire[] to securely communicate," and that the recited "message" must also come from the "second device" and be "receiv[ed], at a network address corresponding to the secure name associated with the first device." The Office has yet to identify any particular alleged "request to communicate" in the token embodiments that is "of the desire[] to securely communicate." (Id. at 80-83; Req. at 214-15.) Accordingly, the rejection should be withdrawn.

The Office alleges that an endpoint having a token-protected alias address corresponds to the "first device associated with a secure name" of claim 1. (Req. at 213.) But in the token embodiments, the alleged "second device" does not perform any functions that correspond to the features assigned to it in the claim. (Supp. Keromytis Decl. ¶ 15.) For example, in the "security token" embodiment of H.235, Endpoint A (the alleged second device) initially sends a regular ARQ message to its gatekeeper to resolve the address of the gateway. (H.235 28.) In the ACF message, the gatekeeper then returns the gateway's address and the security token containing the E. 164 phone number of POTS-B (the alleged first device). (Id.) Next, Endpoint A sends a SETUP message to the gateway with the security token, and the gateway sends the security token back to the gatekeeper for deciphering. (Id. at 28-29.) This ends H.235's disclosure. (See id.) None of these messages is sent from the alleged second device (Endpoint A) and "receiv[ed], at a network address corresponding to the secure name associated with" the alleged first device (POTS-B). (Supp. Keromytis Decl. ¶ 16.) Rather, POTS-B does not receive any message at all in the disclosure ofH.235, let alone a "message ... of the desire[] to securely communicate" from Endpoint A. (Id.)

3PR presents that “Owner's assertions should be disregarded, as the claim language specifies simply that the message be "receiv[ed], at a network address corresponding to the secure name associated with the first device." Patent Owner's argument is thus premised on its mistaken belief that the claims require the message requesting a secure communication link to be received by the first device itself rather than "at a network address corresponding to the secure name associated with the first device." Nothing in the claim language precludes establishment of the secure connection from being mediated by intermediary devices."

The Examiner agrees with the 3PR, as the Patent Owner's contention is based upon an improperly narrow reading of the claim language.

PO argues "The Office's alleged "request to communicate" sent by a calling endpoint (i.e., the alleged second device) in these embodiments further does not correspond to a "message... of the desire[] to securely communicate." In the token embodiments, the calling endpoint never sends a request to communicate, desiring the use of a protective token to a called endpoint. Rather, the tokens are wielded by the called endpoint (i.e., the alleged first device) and used in combination with a gatekeeper so that a calling endpoint cannot obtain the called endpoint's transport address and communicate directly with the called endpoint. (Id. ¶ 17.) Indeed, H.323 describes its tokens as "provid[ing] privacy by shielding an endpoint's Transport Address and Alias address information from a calling party." (H.323 38, emphasis added; see also H.235 28, "Assume that EPA [Endpoint A] is trying to call POTS-B, and POTS-B does not want to expose its E. 164 phone number to EPA," emphasis added.) Called endpoints simply register their tokens with their gatekeepers and use the gatekeepers to shield them from calling endpoints. (H.235 28-29; H.323 38.)"

3PR presents that "Patent Owner's next contention is similarly flawed. Specifically, Patent Owner asserts that the second device does not send a request to securely communicate directly to the first device because the gateway protects that device's addressing information with an access token. Second Response at 36-37. But that assertion is premised on an improper characterization of what the claims actually encompass and ignores that the Office already determined that it is not inconsistent with the claim language for "the gateway [to] act[] and [sic] an intermediary to control access" or for the gateway to "obscure or hide destination addressing information." ACP at 81, 83. This assertion by Patent Owner may therefore be readily dismissed."

The Examiner agrees with the 3PR, as the Patent Owner's contention is based upon an improperly narrow reading of the claim language.

PO argues "The Office and Requester disregard the claim language in asserting that the IPSEC feature of H.235 discloses the above-referenced feature of claim 1. Whereas claim 1 specifically recites "a message from a second device of the desire[] to securely communicate" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device," the Office and Requester incorrectly focus on broad descriptions of "negotiations" between endpoints, such as a request for session initiation "followed then either by an accepted or rejected decision by the other network end." (Second OA at 82-83.) This overbroad and unreasonable analysis overlooks the specific "message" recited in the claim and the various specific claim features related to this "message." A proper analysis reveals that not a single message or step within these "negotiations" in the cited passages of H..323 and H.235

corresponds to "a message from a second device of the desire[] to securely communicate" that is "receiv[ed], at a network address corresponding to the secure name associated with the first device.""

3PR presents that “Patent Owner's challenge to the purported "IPSec-based" rejections suffer from the same flaws. Here, Patent Owner asserts the messages are "either sent from an endpoint to a gateway, or from a gatekeeper to an endpoint--not from the alleged second device to the first device, as required by the claim." Second Response at 38. Once again, the claim language provides only that the message be "receiv[ed], at a network address corresponding to the secure name associated with the first device." The Office properly concluded that the secure connection can be mediated by intermediary devices. ACP at 81, 83. See also Request at 215-16; ACP at 82-83 (explaining that calling endpoint establishes a channel with the receiving endpoint via a gatekeeper, and the endpoints can negotiate a secure channel either during setup or after the connection has been established).”

The Examiner agrees with the 3PR, as the Patent Owner’s contention is again based upon an improperly narrow reading of the claim language.

c.

PO argues “In its previous Response, Patent Owner explained that the Office had not identified any feature within the combined. 323 references that allegedly corresponds to "sending a message over a secure communication link from the first device to the second device." (Id.) The Office still has yet to identify this feature from the combined/-/. 323 references, or otherwise assert that this feature is somehow inherent. (See id. at 84.) For this reason, as well as for the others asserted in Patent Owner's previous Response, the rejection of claim 1 is deficient and should be withdrawn. Net MoneyIN, 545 F.3d at 1369 ("[T]he proponent must show 'that the four corners of a single, prior art document describe every element of the claimed invention.'" (citation omitted)); (Response at 58- 59)."

3PR presents that "The Office correctly maintained its determination that H. 323 discloses "sending a message over a secure communication link from the first device to the second device." ACP at 80-84. In response, Patent Owner argues only that the Office failed to address its arguments in the First Response. Patent Owner is again incorrect. In its prior response, Patent Owner asserted that H.323 did not show a secure communication link between endpoints. This argument rests on the same, incorrect belief that intermediary devices could not broker a secure communication link. First Response at 58-59. The Office properly rejected that assertion by referring to the actual claim language, and noted Patent Owner had offered no new arguments with respect to the "sending" limitation. ACP 81-84. Consequently, the Office fully addressed and rejected Patent Owner's assertions. The rejection of claim 1 was thus proper and should be maintained."

The Examiner agrees with the 3PR, as the Request and the H. 323 disclosure clearly explain that one endpoint receives a request from another endpoint of the desire to communicate securely, and that these endpoint may further be protected by "access tokens," which are utilized to "obscure or hide destination addressing information." Request at 213-17.

2. Independent Claim 2

a.

Patent Owner's argues only for “similar reasons”, and therefore is directed to the above responses by the 3PR and the Examiner.

b.

PO argues “The only address relied upon in the quoted passage of H.323 is a "well-known" transport address relating to a call signalling channel of Endpoint 2. (H.323 50, "well-known Call Signalling Channel Transport Address.") A "transport address" is nothing more than a basic network address with a TSAP identifier. (Id. at 8, defining "transport address.") H.323 does not associate the well-known call signalling channel transport address with any name of an endpoint at all, let alone a "secure name." (Id. at 50.) It is not associated with any particular "secure name," given that H.323 describes it as "well-known." (Id.; Supp. Keromytis Decl. ¶ 24.)”

3PR presents that “In the ACP, the Office correctly maintained its determination that H.323 discloses "a network address associated with the secure name of the second device." ACP at 85-88. In response, Patent Owner repeated its argument that H. 323 does not disclose "a network address associated with the secure name of the second device." Patent Owner's assertion is premised on unclaimed limitations of the claims that would exclude intermediary devices from assisting with establishing a secure connection. The Office properly rejected Patent Owner's assertions when presented previously, and should do so again. ACP at 84-85. The claim language provides only that the "network address" be "associated with the secure name of the second device" and, as the Office found, Patent Owner "attempts to read non-existent limitations into the term 'associated.'" ACP at 86. In the ACP, the Office properly concluded that "the gatekeeper acts and [sic] an intermediary to control access" and "the address of the gateway associated with the second device is sufficient to read on the claim." ACP at 85-86."

The Examiner agrees with the 3PR, as the reference meets the limitation claimed, where the claims do not preclude the use of the central gatekeeper, only providing data transmission between a first device and a second device (further see figures 1 and 2 of the '181 Patent).

c.

PO argues "As discussed above, the Office relies on the IPSEC embodiment ofH.235 to allegedly show "a network address associated with the secure name of the second device," as recited in claim 2. This embodiment involves no "message requesting a network address" or network address resolution, however, since the transport address utilized is already "well-known." (H.323 50.) Thus, to allege disclosure of these claim features, and particularly the feature of "sending a message to a secure name service, the message requesting a network address," the Office switches to the "security token" embodiment. (Second OA at 85-87, citing H.235 28.) By relying on one embodiment involving network address resolution for certain features, and another embodiment not involving any network address resolution for other features, the Office has incorrectly picked and chosen different features from different, inconsistent embodiments, and the rejection of claim 2 should be withdrawn."

3PR presents that "In the ACP, the Office correctly maintained its determination that H.323 discloses the above claim requirements. ACP at 85-88. In response, Patent Owner simply repeats the same assertions it made in its First Response. The crux of Patent Owner's position again rests on unclaimed limitations and features of the claims that would prohibit intermediary devices from assisting with establishing a secure connection. For example, Patent Owner asserts that the Office's construction "incorrectly incorporates ... into the claim... [a] third device: the Gateway." Second Response at 42. Similarly, Patent Owner also contends that the security token embodiment cannot read on the claims because "POTS-B has shielded its alleged 'secure name'--the E. 164 phone number--from Endpoint A with the security token," and thus, Endpoint A cannot "request[] a name associated with POTS-B's E. 164 phone number." Second Response at 42. But the Office has consistently and properly rejected those arguments, explaining that the use of intermediary devices falls within the broadest reasonable construction of the claims. ACP at 85 ("the gateway acts as an intermediary to control access"). Patent Owner also alleges that the Office "pick[s] and choose[s]" features from various unrelated embodiments to satisfy the claims. That assertion rests on the same, incorrect belief that the claims exclude intermediary devices, and therefore the gateway must be considered a first or second device."

The Examiner agrees with the 3PR for reasons previously discussed.

d.

Patent Owner's argues only for "reasons stated above", and therefore is directed to the above responses by the 3PR and the Examiner.

3. Dependent Claims 3-23

Patent Owner's argues only for "reasons discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

4. Dependent Claim 4

PO argues "In its analysis, however, Requester completely ignores the claim language specifying that the "secure name" itself indicates security. As H.323 explains, an access token merely shields an endpoint's alias address or transport address. (H.323 38.) At no point does H.323 describe an access token itself as any type of name or address, and nor does Requester assert that it does. Requester's analysis is irrelevant to the actual claim language, so the rejection should be withdrawn. In the alternative, the Office should reopen prosecution since Patent Owner has not yet had an opportunity in a non-final office action to respond to the new rejection predicated on the "access token" of H. 323. M.P.E.P. § 2673.01(I) ("The patent owner must be given an opportunity to adequately address any change in position adverse to the patent owner's position." (emphasis added)). The Office, meanwhile, argues that a "generic name," such as a phone number or an email address, corresponds to a secure name. (Second OA at 80.) The Office does not assert that a phone number or email address "indicates security," as recited in claim 4, nor does it explain how any other feature might correspond to indicating security. Rather, the Office merely expresses agreement with Requester's access-token argument by stating that with the access token, "these are levels of security, where each of the references desire for layers of securing information show a layering of hidden addresses, encryption, and other means of securing network communications." (Id.) This argument is incorrect for the reasons stated above, and the Office's further argument about various "means of securing network communications" has no bearing on the claim feature providing that "the secure name indicates security."

By persisting with arguments about features outside of the H. 323 naming scheme, the Office fails to identify any secure name that "indicates security." Thus, the rejection of claim 4 should be withdrawn for the reasons stated above and in Patent Owner's previous Response. (Response at 63.) In the alternative, prosecution should be reopened because the Office has adopted a new basis for the rejection, as discussed above. M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed.").

3PR presents that “Patent Owner also incorrectly asserts that the Requester took a "new position" in its Comments by asserting that the "access token" can satisfy the "wherein the secure name indicate security" limitation of claim 4. Second Response at 44. But the use of the access token was clearly identified in the Request and, in fact, Patent Owner addressed this access token in its own First Response. First Response at 63; Request at 220-23 (explaining how a gatekeeper will recognize the addresses and aliases associated with an access token, "as a 'private' alias, knowing that in order to complete the connection it must return the POTS-gateway address "). Similarly, Patent Owner incorrectly contends that the Office took a new position in the ACP that a "generic name"--a "phone number" or "email address"--corresponds to a secure name. The Office's position is neither new nor different from Requester's. In the ACP, the Office explained that the address of the device corresponding to such an email address or phone number could be protected by an access token. ACP at 79-80. It also found that "access tokens, which obfuscate the destination address information, thus indicate security.'" ACP at 88. The Office's and the Requester's positions are not new, and the Office previously conveyed how the limitations of claim 4 are anticipated by H.323."

The Examiner agrees with the 3PR.

5. Dependent Claim 5

PO argues "the Office's arguments in the Second Office Action only addressed the "security token" and "access token" embodiments, whereas the maintained rejection of claim 5 relied exclusively upon the IPSEC feature ofH.235. (Id. at 86-87; Req. at 227-28.) The Office did not address any of Patent Owner's arguments with respect to the IPSEC embodiment for the "receiving a message . . ." feature of claim2.

(Second OA at 86-87; see Response at 61-62.) Neither did Requester. (Comments at 33-34.) Thus, the Office dismisses Patent Owner's arguments as unpersuasive while purporting to have already addressed them, but the Office in fact never addressed those arguments. Rather, it abandoned its earlier position regarding the IPSEC embodiment with respect to the "receiving a message . . ." feature of claim 2 in the Second Office Action. (Compare Second OA at 86-87; Comments at 33-34 with Req. at 222-24.)

Because the Office no longer relies on the IPSEC embodiment ofH.235 after Patent Owner's previous Response regarding the feature of "receiving a message..." recited in claims 2 and 5, the rejection of claim 5--predicated exclusively on this same IPSEC embodiment--should be withdrawn."

3PR presents that "In the ACP, the Office correctly determined that H.323 anticipates every limitation of dependent claim 5. ACP at 89. In response to the First Action, Patent Owner argued that H.323 "fail[s] to disclose 'receiving a message containing the network address associated with the secure name of the second device,' as received in claim 2. For the additional claim 5 feature... the address returned in the IPsec passage corresponds to a 'call signaling channel,' rather than the endpoint earlier identified as the 'second device .... '" First Response at 63. In the ACP, the Office rejected that argument, observing that Patent Owner had improperly imported unclaimed limitations into claim 2 prohibiting the use of intermediary devices. ACP at 84-85, 89. In its Second Response, Patent Owner presents the same arguments. Because they continue to be based on unclaimed limitations and features of the claims, they should continue to be rejected. In addition, Patent Owner argues the Office has failed to address its arguments relating to the "IPsec embodiment." But, as explained above under claim 2, this argument is based on Patent Owner's misunderstanding of the H-series processes; IPsec is not a separate embodiment, but an optional feature that can be implemented to work with the security tokens ofH.323. Accordingly, the Office's rejection of claim 5 over H. 323 was proper and should be maintained."

The Examiner agrees with the 3PR that the reference uses layered security measures to meet a certain level of security that all security measures combined provide.

6. Dependent Claim 9

PO argues "The Office and Requester do not show how the combined H.323 references disclose "automatically initiating the secure communication link after it is enabled." (Second OA at 89.) Requester argues that the mere feature of "dynamically" updating an endpoint's security policy within the IPSEC embodiment corresponds to these claim features. (Id.) But at that point in the IPSEC embodiment, no secure communication link is being initiated, let alone already been "enabled," as recited within the claim. (Supp. Keromytis Decl. ¶ 26.) H.235 explains that the endpoints continue to have significant non-automatic authentication hurdles before any IPSEC-protected communications are enabled or subsequently initiated. (H.235 30.) For example, H.235 specifies that "person-to-person Q&A" and "user-to-user authentication" are involved in negotiating the characteristics of the channel "before any H.245 packets are transmitted." (Id.) The Office does not supplement Requester's deficient argument, and, accordingly, the rejection should be withdrawn."

3PR presents that "In the ACP, the Office correctly found that H.323 anticipates dependent claim 9. ACP at 89-90. In its First Response, Patent Owner asserted simply that "Requester makes the conclusory assertion that any alleged communication link would be initiated automatically." First Response at 64. In response to the ACP, Patent Owner now expands on its assertions, arguing that the literal absence of the words "automatically initiating" in H. 323 means that a secure communication link established would not occur automatically upon completion of negotiation process between networked devices. Second Response at 46. Patent Owner's argument adds nothing new to its previous position, and the Office can reject it on the same basis as it did previously. Patent Owner also incorrectly describes H.323. As explained in the Request, First Comments, and ACP, H. 323 explains that "[a]fter obtaining the address and port number of the call signaling channel, the calling endpoint would dynamically update its security policy to require the desired IPSEC security on that address and protocol/port pair." Request at 219. The Office correctly determined these steps occur automatically without any further user interaction. ACP at 90. Accordingly, H. 323 discloses the limitations of claim 9, and the Office's rejection of claim 9 was proper and should be maintained."

The Examiner agrees with the 3PR, as the "dynamically update" happens without further users action.

7. Dependent Claims 10 and 11

Patent Owner's argues only for reasons discussed above, and therefore is directed to the above responses by the 3PR and the Examiner.

8. Dependent Claim 13

PO argues “Claim 13 incorporates the features of claim 2, "wherein the receiving and sending of messages through the secure communication link includes multiple sessions." Patent Owner previously rebutted this rejection by arguing that the feature relied upon by the Office would require setting up separate logical channels, which is inconsistent with the singular "secure communication link" recited in the claim. (Response at 64.) Having previously relied upon a single H.245 channel within the IPSEC embodiment as corresponding to the "secure communication link" of claim 2, Requester now dramatically expands its interpretation of "secure communication link" to include many such channels. (Second OA at 91-92.) Nowhere does Requester attempt to justify its dramatic expansion of the plain claim language, instead claiming that any limitations on the singular claim term "secure communication link" are "non-existent." (Id.) Any broadest reasonable interpretation of the claims must be "consistent with the specification," but Requester does not attempt to find support in the specification for its interpretation contrary to the actual claim language. Abbott, 696 F.3d at 1148; M.P.E.P. § 2258(I)(G). Because the Office's rejection depends on

Requester's deficient arguments, the rejections should be withdrawn for the reasons discussed above and in Patent Owner's previous Response. (Response at 64.)"

3PR presents that "In the ACP, the Office correctly found that H.323 discloses every limitation of claim 13, which specifies that the "receiving and sending of messages through the secure communication link includes multiple sessions." ACP at 91. In its Second Response, Patent Owner makes the same argument it made in its First Response, namely that H.323 employs separate channels and separate sessions and that claim 13 includes one secure communication link and separate sessions. Second Response at 47; First Response at 64. In the ACP, the Office found that H.323 provided for the use of multiple sessions and that nothing in the claims limited the multiple sessions to the same secure communication link. ACP at 92. The Office correctly disregarded Patent Owner's incorrect assertions. Accordingly, the rejection was proper and should be maintained."

The Examiner agrees with the 3PR, as the claim language "wherein the receiving and sending of messages through the secure communication link includes multiple sessions" does not limit the sessions to the same communication link.

9. Dependent Claim 21

Patent Owner's argues only for "the same reasons", and therefore is directed to the above responses by the 3PR and the Examiner.

10. Independent Claim 26 and Dependent Claim 27

PO argues “The Office dismisses Patent Owner's arguments as allegedly "present[ing] no response that is distinct from those answered above." (Second OA at 92.) The Office is incorrect. As explained in Patent Owner's previous Response, the Office has not shown how H.323 allegedly discloses "an unsecured name associated with the first device" and a "unique network address correspond[ing] to the secure name associated with the first device." (Response at 65.) The Office did not address these features in any previous part of its H.323 section in the Second Office Action. Thus, the rejection should be withdrawn for the unrebutted reasons stated in Patent Owner's previous Response. (Id.) Moreover, it is incorrect for the Office to adopt a rejection, dismiss Patent Owner's arguments as previously addressed when in fact they were not addressed, and then maintain the rejection and close prosecution. An ACP is only permitted "[u]pon consideration of the issues a second or subsequent time." 37 C.F.R. § 1.949; see also M.P.E.P. § 2671.02. Prosecution should be reopened because Patent Owner's arguments have not yet been considered, and the rejection should be withdrawn for the reasons stated above and in Patent Owner's previous Response. (Response at 65.)”

3PR presents that “In the ACP, the Office correctly maintained its determination that H.323 anticipates each and every limitation of claims 26 and 27. ACP at 92. In response to the First Action, Patent Owner presented no response distinct from its response to the rejection of claims 1 and 2. In response to the ACP, Patent Owner now complains that the Office did not respond to its argument that H. 323 does not disclose a "unique network address" as required by the claims. Patent Owner is wrong. In confirming the rejections of claims 1 and 2, the Office gave an in- depth explanation of how H.323 anticipates the claims. ACP at 79-88. In particular, it explained how a gatekeeper in the H. 323 scheme could be associated with one device and how a device could register one secure name and one unsecured name with the gatekeeper, thus satisfying the "unique network address correspond[ing] to the secure name associated with the first device" element of the limitations. ACP at 81-83. The Office's findings also are consistent with Patent Owner's reading of a "unique network address" in concurrent litigation, in which, Patent Owner has asserted "[a] prospective FaceTime caller must also request and obtain registration of a secure name associated with the caller's device through the FaceTime system .... [A] certificate assures that the name of the caller's (first) Accused Device is secure. This secure name corresponds to the unique network address of the caller's (first) Accused Device .... To call someone using FaceTime, you need their phone number or email address. Exhibit A at 14-15. Thus, because Patent Owner has maintained that an email address or phone number secured by a certificate can "correspond to the unique network address" associated with the first device, its arguments to the contrary should be given no weight by the Office. The Office correctly addressed and dismissed each of Patent Owner's unpersuasive arguments."

The Examiner agrees with the 3PR, as a gatekeeper in the H. 323 scheme may be associated with one device where a device registers one secure name and one unsecured name with the gatekeeper, thereby providing a "unique network address correspond[ing] to the secure name associated with the first device".

11. Independent Claims 24 and 28 and Dependent Claims 25 and 29

Patent Owner's argues only for "reasons similar to those discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

IX. The Rejection of Claims 1-29 under Johnson (ISSUE 13)

Overview of Johnson

Johnson teaches a secure name being registered by the secure mail server with the secure name server. (see column 10, lines 36-52). Johnson discloses that the a first device securely communicated with the secure name server in order to request a network address that is associated with the secure name--which is associated with the network address---of the second device, i.e., the secure mail server. At 11:21-37, Johnson explains: *Process to Get an Address from a Secure Name Server FIG. 7 of the drawings outlines the process by which an unknown address, such as* ***the dynamic address of a secure mail server, is obtained from a secure name server.*** *The process starts by selecting the target secure name server machine by its fixed address/name as shown in block 150. The user then provides the secure name server with its logon protocol combination as shown at block 152. If the user logon combination is verified then a session is established with a secure name server as shown at block 154. ...if the session has been correctly established as shown at block 156, then the user will be allowed to request the address for the named machine at the client site as shown at block 158.*

1.

a.

PO argues “Requester and the Office advance two constructions for the term "secure name." (Comments at 37-38; Second OA at 94-96.) The first relies on out-of-context external statements while failing to consider the '181 patent specification itself. (Comments at 37-38; Second OA at 94-95.) The second is Requester's own construction, adopted by the Office. (Comments at 37-38; Second OA at 95-96.) A proper analysis discloses that the secure mail server's name does not satisfy either of these flawed constructions.

3PR presents that “In response to the ACP, Patent Owner states that "the term 'secure name' refers to those names used to communicate securely that are resolved by a secure name service, consistent with its statements during prosecution." Second Response at 49. However, it repeats its arguments that embodiments in the ' 181 specification additionally require a "secure name server" to "further support establishing a secure communications link" and that Johnson discloses a conventional name server that does not. Second Response at 49; First Response at 68. The Office correctly rejected this argument in the ACP, observing that Johnson's secure name server implements security features that make it distinct from a conventional name server. ACP at 95. Also, in the First Action, the Office found that the broadest reasonable construction of "secure name service" requires only that it be able to resolve a "secure name" to distinguish it from a conventional name server. Order at 5. The Office properly rejected Patent Owner's contentions that the claims should be read as implicitly requiring more, in part because those statements are inconsistent with Patent Owner's prior representations to the Office. ACP at 94-95.

The Examiner agrees with the 3PR, as Johnson positively recites subsequent to a user being identified / logged on, a session (secure link) is established through the secure name server.

PO argues “Patent Owner does no such thing. As discussed in detail in Patent Owner's previous Response, Johnson does not teach or suggest that the name of the secure mail server requires authorization to access or that it is protected through encryption. (Response at 68.) Instead, Johnson teaches that the user knows the name of the secure mail server, but never discusses whether the user required authorization to access the name or whether the name was protected through encryption during access. (See, e.g., Johnson 7:12-17, 9:25-27; Keromytis Decl. ¶ 122.)”

3PR presents that “Patent Owner also repeats the argument from its First Response that Johnson does not disclose a "secure name," asserting that the name used to access Johnson's secure mail server cannot be secure because users know the name in advance. The Office properly addressed and rejected that argument in the ACP, explaining that "the user at the first device requests access to the secure mail server via a 'name' (secure) then when they are authenticated via the secure name service, they are provided with the 'address' (unsecure) corresponding to the provided 'name.'" ACP at 96, 98. The Office correctly observed that the secure name server can require authentication before returning the corresponding network address and the mail server's name can only be resolved by the secure name server; thus the server's name is a "secure name" within the meaning of the claims. The Office thus properly confirmed that Johnson discloses the above listed features of claim 1."

The Examiner agrees with the 3PR, as previously stated in the ACP "the user at the first device requests access to the secure mail server via a 'name' (secure) then when they are authenticated via the secure name service, they are provided with the 'address' (unsecure) corresponding to the provided 'name.'" ACP at 96, 98

b.

PO argues "In the First Office Action, the Office conceded that Johnson did not disclose the claimed "unsecured name," and looked to Johnson in combination with either RFC 2131 or RFC 1034 to meet the claims. (First OA at 12, incorporating by reference the Request at 270-318.) But in an about-face, the Office now additionally contends that the dynamic address of the secure mail server in Johnson alone corresponds to the "unsecured name." The Office is incorrect. Moreover, because Johnson teaches away from the address allocation and registration of RFC 2131 and because one of ordinary skill in the art would not have been motivated to combine the secure communication system of Johnson with the open-access DNS system of RFC 1034, Johnson in view of RFC 2131 and RFC 1034 also does not disclose the claimed "unsecured name."

Contrary to the Office's contentions, the dynamic address of the secure mail server does not correspond to the claimed "unsecured name." As Johnson explains, the dynamic address is an "Internet protocol address" and not a "name" at all. (Johnson 6:27-29.)”

3PR presents that “The Office has not changed its position. The Request, which the Office incorporated by reference, explained that "the name of the secure mail server is a secure name" and it "has its own unique IP address" as well as "a domain name registered in the public DNS system and/or a client identifier associated with such domain name that constitutes an 'unsecured name.'" Request at 274. The Request clearly identified the mail server's address as an unsecured name. Patent Owner's contention this is somehow "new" is thus false.”

…

3PR presents that “As the Request explained, Johnson discloses that the secure name server may be used in many applications, e.g., interbusiness network communication, and it would have been obvious and necessary to register the secure name server with the public DNS system to enable such communications. Request at 272-74.”

…

3PR presents that “Patent Owner also contends that "an 'Internet protocol address' [is] not a 'name' at all." Second Response at 50. That contention should be disregarded as being inconsistent with Patent Owner's prior representations that distinguish a "secure name" from a conventional name. An IP address, especially one associated with a registered domain name, is a conventional name and it is publicly accessible."

The Examiner agrees with the 3PR, as the position has remained the same form the original request. Furthermore, these IP addresses are distinguishing titles provided to mark a specific destination, where according to Patent Owners own previous description of network addresses being name based (see column 7, lines 24-36).

PO argues "Johnson teaches away from using the Dynamic Host Configuration Protocol of RFC 2131. RFC 2131 teaches the following:

> DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "manual allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client.

(RFC 2131 2.) Johnson does not rely on any of these methods to assign a dynamic address to the secure mail server. According to Johnson, "the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network." (Johnson 6:26-27.) Unlike the "manual allocation" defined in RFC

2131, Johnson identifies no DHCP server to convey the address to the secure mail server from the network.

3PR presents that “Patent Owner also argues that Johnson teaches away from RFC 2131 because Johnson "does not rely on any of the[] methods [described in RFC 2131] to assign a dynamic address to the secure mail server." Patent Owner's argument is based on a misreading of Johnson. Johnson explains "the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network." While Patent Owner contends this teaches away from using DHCP, in fact it does not. Instead, Johnson discloses that when the mail server connects to the network, the network assigns it a dynamic address - that is exactly how DHCP works. The Office may thus disregard Patent Owner's contention that "Johnson identifies no DHCP server to convey the address to the secure mail server from the network." Second Response at 51.”

The Examiner agrees with the 3PR, as RFC 2131 is not so limited to manual or automatic allocation but further supports the dynamic allocation, and the mere fact that Johnson does not specifically point out that the dynamic address is obtained from a DHCP server does not preclude use of RFC 2131.

PO argues “the problems and solutions proposed by Johnson and RFC 1034 are diametrically opposed. While Johnson is concerned with security and the prevention of public access to communications across network systems, (Johnson 1:20-28), Requester admits that RFC 1034 is directed to improving and expanding public access to communications using a user-friendly naming scheme, (Comments at 40). Discussing security, Johnson explains that "the remote administrator 20 will establish logon protocol for users to access the secure name server 14," which it will pass on to users of the protected communication network such that "only users authorized by the remote administrator 20 will be allowed to access the secure name server 14." (Johnson 6:50-59.) In light of Johnson's stated intention of limiting access for security purposes, it makes little sense for the servers of Johnson to register domain names in the public DNS to expand access. Because the proposed combination of Johnson with RFC 1034 would undermine Johnson's intended purpose, the rejection should be withdrawn. See M.P.E.P. § 2143.01."

3PR presents that "Finally, Patent Owner argues that Johnson's intention is to "limit access for security purposes" and it would make little sense for servers of Johnson to register domain names in the public DNS to expand access. However, Patent Owner fails to explain how these purposes are "diametrically opposed" since one of ordinary skill would have appreciated Johnson's intention of developing a flexible system, capable of providing secure communications both within a network and across networks via public resources such as the Intemet. The combination does not compromise security or the intended purpose of Johnson."

The Examiner agrees with the 3PR, as the combination would be an expansion of the features of Johnson not a contradiction.

B. Independent Claim 2

Patent Owner's argues only for reasons “discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

C. Dependent Claims 3-16 and 18-23

Patent Owner's argues only for “reasons discussed above”, and therefore is directed to the above responses by the 3PR and the Examiner.

D. Dependent Claim 3

PO argues “Both Requester and the Office contend that one of ordinary skill in the art would have been motivated to modify the secure name server of Johnson to register with a public DNS, "making it possible to locate the secure name server 14 by name, for example, through the public resources of the Internet," as purportedly taught by RFC 1034. (Comments at 40, emphasis added; Second OA at 100-02.) By this reasoning, registering the secure name server 14 with a public DNS would convert what Requester and the Office claim is an "unsecured name" associated with the server to a "secure domain name." Even if one were to incorrectly assume that the secure name service and secure mail service are located on the same machine in the manner Requester and Office claim, (Req. at 277; First OA at 12, incorporating by reference the Request at 270-318), registering the purported "unsecured name" of the secure name server 14 with a public DNS does not somehow produce a "secure domain name" (emphases added). In other words, the purported "secure name" of the secure mail server 16 would not become a "secure domain name" by making it easier to locate the secure name server 14 publicly."

3PR presents that "in response to the ACP, Patent Owner belatedly asserts that Johnson in view of RFC 1034 "does not somehow produce a 'secure domain name'." Second Response at 52-53. The Office should disregard this comment as it is untimely presented. Even if considered, it should be disregarded as being unpersuasive. As the Request explained, a person of ordinary skill in the art would have found motivation within Johnson to incorporate mechanisms to facilitate inter-business communications by, for example, making it possible to locate the secure name server 14 by name through the public resources of the Intemet. Patent Owner's new argument is based on its misconception that Johnson does not show a "secure name" and an "unsecured" name which, as explained above. See also Request at 273-74, 282- 84."

The Examiner agrees with the 3PR, as motivation has been shown to make Johnsons system accessible over the internet.

E. Dependent Claims 9-11 and 13-16

PO argues "as discussed in Patent Owner's previous Response, one of ordinary skill in the art would not have combined the two references at least because combining the two would change the principle of operation in the Johnson system and render Johnson unsatisfactory for its intended purpose. (Response at 72-73.) Requester and the Office respond that the security mechanisms of Johnson would simply be modified to include the additional security mechanisms of RFC 2401. (Comments at 41; Second OA at 103-04.) Yet this would fundamentally change the principle of operation in Johnson. According to Johnson, the prior art "suffer[s] from the drawbacks of using known communication pathways, having known addresses, and some systems even transfer secure key information over the communication lines." (Johnson 4:55-59.) Johnson therefore advocates a method in which key information is not transmitted over the communication line. (Id. at 4:60-63, stating that "there is a need for an improved communication method which allows for encrypted information transfer to dynamic locations without transmitting the keys over the communication line.") The system taught in RFC 2401, however, involves sending security and key management traffic (i.e., ISAKMP) between the hosts and across the communication lines. (RFC 2401 17, stating that "[t]he SPD is used to control the flow of ALL traffic through an IPsec system, including security and key management traffic (e.g., ISAKMP) from/to entities behind a security gateway," 25, stating "a requirement for a security gateway to be configurable to pass IPsec traffic (including ISAKMP traffic) for hosts behind it.") Modifying Johnson with RFC 2401 would vitiate the very improvement Johnson advocates. As a result, the proposed combination of Johnson with RFC 2401 would change the principle of operation in Johnson, and the rejections are accordingly incorrect. See M.P.E.P. § 2143.01."

3PR presents that "As explained in the ACP, a person of ordinary skill in the art would have found motivation within Johnson to incorporate additional security mechanisms for communications over the Internet, such as interbusiness network communications. ACP at 103-04 (citing Request at 289-90). That person would have found in Johnson or RFC 2401 identification of the same problem (improving security for Internet Protocol communications) as well as a solution to the same problem: an encryption and/or tunneling scheme. There is nothing in either reference that suggests that one must modify the essential features of the Johnson systems or change its principle of operation to implement IPSec in communications."

The Examiner agrees with the 3PR, as the combination would be an expansion of the features of Johnson not a contradiction, where both solve similar problems as far as securing IP communications, only in supplementary manners.

F. Dependent Claim 21

Patent Owner's argues only for reasons "discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

G. Independent Claims 24, 26, 28, and 29

Patent Owner's argues only for reasons "discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

H. Dependent Claims 25 and 27

Patent Owner's argues only for "reasons discussed above", and therefore is directed to the above responses by the 3PR and the Examiner.

X. Secondary Consideration Weigh Against Obviousness

The Patent Owner argues that "the claimed inventions... addressed a long-felt need".

The Examiner respectfully submits that Patent Owner appears to show that the prior art is nothing more than a generic systems using a name server to properly route alternately named network traffic. The references however, provide an advanced naming scheme allowing the IP address of the recipient to be hidden to ensure secure communication, while providing a date that predates that of the '181 Patent.

The Patent Owner argues that "the claimed inventions... succeeded where others have failed".

The Examiner respectfully submits that this is the goal of this reexamination to prove or disprove this point, in view of the substantial new question of patentability of the claimed invention. In this case, though the noted DARPA, CIA, and SAIC projects appear to have failed, the references noted above appear to have succeeded in implementing the claimed invention.

The Patent Owner argues that "the claimed inventions... have been commercially successful".

The Examiner respectfully submits that the evidence of commercial success is not convincing as there is no one to one mapping between the claims and what is taught in the Short disclosure, as it is unclear whether the infringement / licensing agreements had anything to do with the claimed subject matter. The mere fact that a product using the general idea of the claimed invention has had commercial success does not necessarily make the claimed invention novel.

To be given substantial weight in the determination of obviousness or nonobviousness, evidence of secondary considerations must be relevant to the subject matter as claimed; in this case the Examiner does not see a nexus between the merits of the claimed invention and the evidence of secondary considerations.

The Patent Owner argues that "the claimed invention... received praise from others in the field".

The Examiner respectfully submits that the Short disclosure shows a secure method for conducting network communication, where the references applied supra are directed at the same or similar improvements, with an earlier filing date.

Secondary Considerations

The evidence of secondary considerations presented during prosecution has been reconsidered against the underlying evidence supporting the findings of obviousness listed above. After reweighing all of the available evidence, the examiner finds that the secondary considerations do not overcome the evidence supporting the conclusions of obviousness

Conclusion

This is a RIGHT OF APPEAL NOTICE (RAN); see MPEP § 2673.02 and § 2674. The decision in this Office action as to the patentability or unpatentability of any original patent claim, any proposed amended claim and any new claim in this proceeding is a FINAL DECISION.

No amendment can be made in response to the Right of Appeal Notice in an *inter partes* reexamination. 37 CFR 1.953(c). Further, no affidavit or other evidence can be submitted in an *inter partes* reexamination proceeding after the right of appeal notice, except as provided in 37 CFR 1.981 or as permitted by 37 CFR 41.77(b)(1). 37 CFR 1.116(f).

Each party has a **thirty-day or one-month time period, whichever is longer,** to file a notice of appeal. The patent owner may appeal to the Board of Patent Appeals and Interferences with respect to any decision adverse to the patentability of any original or proposed amended or new claim of the patent by filing a notice of appeal and paying the fee set forth in 37 CFR 41.20(b)(1). The third party requester may appeal to the Board of Patent Appeals and Interferences with respect to any decision favorable to the patentability of any original or proposed amended or new claim of the patent by filing a notice of appeal and paying the fee set forth in 37 CFR 41.20(b)(1).

In addition, a patent owner who has not filed a notice of appeal may file a notice of cross appeal within fourteen days of service of a third party requester's timely filed notice of appeal and pay the fee set forth in 37 CFR 41.20(b)(1). A third party requester who has not filed a notice of appeal may file a **notice of cross appeal within fourteen days of service** of a patent owner's timely filed notice of appeal and pay the fee set forth in 37 CFR 41.20(b)(1).

Any appeal in this proceeding must identify the claim(s) appealed, and must be signed by the patent owner (for a patent owner appeal) or the third party requester (for a third party requester appeal), or their duly authorized attorney or agent.

Any party that does not file a timely notice of appeal or a timely notice of cross appeal will lose the right to appeal from any decision adverse to that party, but will not lose the right to file a respondent brief and fee where it is appropriate for that party to do so. If no party files a timely appeal, the reexamination prosecution will be terminated, and the Director will proceed to issue and publish a certificate under 37 CFR 1.997 in accordance with this Office action.

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving this patent throughout the course of this reexamination proceeding. The requester is also reminded of the ability to similarly appraise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP § § 2607, 2682, and 2686.

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

By Mail to: Mail Stop Ex Parte Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/Dennis G. Bonshock/

Primary Examiner, Art Unit 3992

Conferee: /Mary Steelman/

Primary Examiner, CRU 3992

/Alexander J Kosowski/

Supervisory Patent Examiner, Art Unit 3992

Notice of References Cited	Application/Control No. 95/001,949	Applicant(s)/Patent Under Reexamination 8051181	
	Examiner DENNIS BONSHOCK	Art Unit 3992	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	Response/Amendment, Serial No.: 11/679,416 (EXHIBIT A-28)
*	V	VIRNETX INC. vs. CISCO SYSTEMS, INC., Final Judgment Pursuant to FED.R.CIV.P.54(b), Case No. 6:10-CV-417, (EXHIBIT A-30)
*	W	VIRNETX INC. vs. APPLE, INC., Verdict Form, CASE NO. 6:10-CV-417 (EXHIBIT A-10)
*	X	In re Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing Same, Patent Owner's Evidence of Infringement against Requester, ITC investigation 337-TA-858, U.S. PATENT NO. 8,051,181 (EXHIBIT A / EXHIBIT 13)

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95001949	8051181
	Examiner	**Art Unit**
	DENNIS BONSHOCK	3992

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
Reviewed all prosecution history	5-22-12	dgb
Reviewed all prosecution history	1-3-13	dgb
Reviewed all prosecution history	7-2-13	dgb

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Reexamination	**Application/Control No.** 95001949	**Applicant(s)/Patent Under Reexamination** 8051181
	Certificate Date	**Certificate Number**

Requester Correspondence Address: □ **Patent Owner** ☒ **Third Party**

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

LITIGATION REVIEW ☒	DGB (examiner initials)	05/23/2012 (date)
Case Name		Director Initials
VirnetX Inc. v. Cisco Systems, Inc., Apple, Inc., et al., Civ		

COPENDING OFFICE PROCEEDINGS

TYPE OF PROCEEDING	NUMBER

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
) Control No.: 95/001,949
Victor Larson et al.)
) Group Art Unit: 3992
U.S. Patent No. 8,051,181)
) Examiner: Dennis G. Bonshock
Issued: November 1, 2011)
) Confirmation No.: 4522
For: METHOD FOR ESTABLISHING SECURE)
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE) **VIA EFS WEB**
NETWORK

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S NOTICE OF APPEAL UNDER 37 C.F.R. § 41.61

Pursuant to the Right of Appeal Notice dated August 16, 2013, VirnetX Inc., the owner of U.S. Patent No. 8,051,181 ("the '181 patent") appeals to the Patent Trial and Appeal Board all pending rejections of the claims, including claims 1-29 of the '181 patent. The required fee of $800.00 is being submitted herewith.

Please grant any extensions of time required to enter this paper and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 16, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U.S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Notice of Appeal Under 37 C.F.R. § 41.61 was served by first-class mail on September 16, 2013, on counsel for the third party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 16, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Joseph Edwin Palys./Sheryl Lewis
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of Appeal	1401	1	800	800
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**800**

Electronic Acknowledgement Receipt

EFS ID:	16859540
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	16-SEP-2013
Filing Date:	28-MAR-2012
Time Stamp:	12:29:55
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$800
RAM confirmation Number	10965
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

<table>
<tr><td>1</td><td></td><td>181ReexamNoticeofAppeal.pdf</td><td>83101
3dd5331fa1af1989d8f5dd631ddaa49acd1bd65c</td><td>yes</td><td>2</td></tr>
<tr><td rowspan="4"></td><td colspan="5"><b>Multipart Description/PDF files in .zip description</b></td></tr>
<tr><td colspan="3"><b>Document Description</b></td><td><b>Start</b></td><td><b>End</b></td></tr>
<tr><td colspan="3">Reexam Miscellaneous Incoming Letter</td><td>1</td><td>1</td></tr>
<tr><td colspan="3">Reexam Certificate of Service</td><td>2</td><td>2</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>2</td><td>Fee Worksheet (SB06)</td><td>fee-info.pdf</td><td>30140
a2301789c6029e55d9139f0ce7856487233c9f6b</td><td>no</td><td>2</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td colspan="4"><b>Total Files Size (in bytes):</b></td><td colspan="2">113241</td></tr>
</table>

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U.S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE
COMMUNICATION LINK BETWEEN
COMPUTERS OF VIRTUAL PRIVATE
NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S PETITION FOR AN EXTENSION OF TIME TO FILE AN APPEAL BRIEF

VirnetX Inc., the owner of U.S. Patent No. 8,051,181 ("the '181 patent"), files this petition under 37 C.F.R. § 1.183 and M.P.E.P. § 2673.02, and requests that the Director waive or suspend the requirements of 37 C.F.R. § 41.66(a), prohibiting an extension of time for filing an appeal brief. Consistent with the procedure recommended in MPEP § 2673.02, VirnetX also requests an extension of time for filing its appeal brief until the later of (1) one month after the Director decides VirnetX's Petition Seeking Review of Decision Denying Patent Owner's Petition to Reopen Prosecution ("Petition Seeking Review"), or (2) one month after VirnetX's appeal brief would otherwise be due. VirnetX requests the extension so the Director can decide the Petition Seeking Review, which may eliminate the need for filing an appeal brief entirely.

To avoid unnecessarily burdening the Office and the parties with preparing, filing, and processing appeal briefs that may become moot if the Office reopens prosecution and the rejections are altered or withdrawn, VirnetX respectfully requests an extension of time to file its appeal brief.

To the extent entry and consideration of this petition requires suspension of any rules in addition to 37 C.F.R. § 41.66(a), VirnetX requests such a suspension under 37 C.F.R. § 1.183. The petition fee is being submitted concurrently with this Petition. Please charge any additional fee due or credit any overpayment in connection with the filing of this Petition to Deposit Account No. 06-0916.

I. BACKGROUND

Third-party requester Apple Inc. ("Apple") filed a Request for Reexamination ("Request" or "Req.") on March 28, 2012. The Office granted the Request and issued a first Office Action on June 4, 2012, incorporating by reference nearly all of the Request. VirnetX filed a response ("Response") to the first Office Action on September 4, 2012. Apple filed third-party comments ("Comments") to VirnetX's Response on October 22, 2012. The Office subsequently issued an Action Closing Prosecution ("ACP") on January 16, 2013, maintaining each of the rejections adopted in the first Office Action.

On March 18, 2013, VirnetX petitioned the Office to reopen prosecution. In the Petition, VirnetX explained that the ACP provided new bases for its rejections by, among other things, switching and relying on different features in the references that were not previously relied upon in the initial Office Action. (Petition 2-7.) The Office denied VirnetX's Petition in its Decision on May 28, 2013. VirnetX petitioned for review of this decision on July 9, 2013. The Director has not yet rendered a decision on this Petition for Review. Nonetheless, the Office issued a

Right of Appeal Notice ("RAN") on August 16, 2013, and VirnetX filed a Notice of Appeal on September 16, 2013.

II. ARGUMENT

VirnetX requests an extension of time because a decision by the Director on VirnetX's Petition for Review may result in reopening prosecution, which would avoid the need to file an appeal brief. The extension would therefore conserve the resources of the Office, Requester, and VirnetX.

Granting an extension is also consistent with the procedure set forth in M.P.E.P. § 2673.02, which recommends seeking waiver of the prohibition of an extension of time to file an appeal brief while awaiting a decision on a petition to enter an amendment into the record. This case is analogous to the situation contemplated by the M.P.E.P. because, in both scenarios, the Director's decision could significantly alter the scope and content of any appeal. In the § 2673.02 scenario, the amendment could alter the scope of the claims. Similarly, reopening prosecution in this case could result in introduction of further evidence to rebut the Office's rejections, as detailed in the Petition Seeking Review. It may also result in the Examiner withdrawing previously maintained rejections. Thus, VirnetX's request is consistent with the procedure outlined in § 2673.02.

An extension here is also consistent with prior Board decisions addressing similar circumstances. For example, the Office granted a one-month extension of time to obtain the result of a decision on a petition to enter an expert declaration into the record. (*See* Control No. 95/001,788, Decision on Petition for Waiver of Timing Requirements in Reexamination at 2 (Sept. 19, 2013).) The decision noted that, in the event VirnetX "were to have filed a paper merely to keep the proceeding pending, in this case, that filing would cause unnecessary expenditure of resources by the Central Reexamination Unit (CRU) to consider a paper that could become moot, should the petition be granted." (*Id.*; *see also* Control No. 95/001,789, Decision on Petition for Waiver of Timing Requirements in Reexamination at 2 (Sept. 19, 2013).) The same reasoning applies here, as requiring briefing to proceed before the Director decides the Petition Seeking Review would not only result in an unnecessary expenditure of resources regarding VirnetX's appeal brief, but would also trigger deadlines for other briefs, such as Apple's respondent brief. Thus, without the extension, the Office may need to unnecessarily expend resources on multiple papers that could become moot.

To avoid the need for continued petition practice, VirnetX proposes that it would be most efficient to extend the time for filing its appeal brief until a month after the Director decides VirnetX's Petition Seeking Review. If the Director prefers not to link the appeal-brief deadline to the decision dates of VirnetX's other petition, VirnetX alternatively requests a one-month extension of time after VirnetX's appeal brief would otherwise be due. This would most efficiently conserve the resources of the Office, Requester, and VirnetX, particularly considering the many concurrent proceedings requiring attention from VirnetX and the Office.[1]

[1] VirnetX is also currently involved in the following 10 related reexamination proceedings: Control Nos. 95/001,679 and 95/001,682 involving U.S. Patent No. 6,502,135; Control Nos. 95/001,697 and 95/001,714 involving U.S. Patent No. 7,490,151; Control No. 95/001,746 involving U.S. Patent No. 6,839,759; Control Nos. 95/001,788 and 95/001,851 involving U.S. Patent No. 7,418,504; Control Nos. 95/001,789 and 95/001,856 involving U.S. Patent No. 7,921,211; and Control No. 95/001,792 involving U.S. Patent No. 7,188,180.

VirnetX is additionally involved in the following 11 related *inter partes* review proceedings: IPR2013-00348 involving U.S. Patent No. 6,502,135; IPR2013-00349 involving U.S. Patent No. 6,502,135; IPR2013-00354 involving U.S. Patent No. 7,490,151; IPR2013-00375 involving U.S. Patent No. 6,502,135; IPR2013-00376 involving U.S. Patent No. 7,490,151; IPR2013-00377 involving U.S. Patent No. 7,418,504; IPR2013-00378 involving U.S. Patent No. 7,921,211; IPR2013-00393 involving U.S. Patent No. 7,418,504; IPR2013-00394 involving U.S. Patent No. 7,418,504; IPR2013-00397 involving U.S. Patent No. 7,921,211; and IPR2013-00398 involving U.S. Patent No. 7,921,211.

III. CONCLUSION

For these reasons, VirnetX requests that the Director suspend the requirements of 37 C.F.R. § 41.66(a), which prohibits an extension of time for filing an appeal brief. VirnetX also requests that the Director grant an extension of time for filing its appeal brief until one month after the Director decides VirnetX's Petition Seeking Review of Decision Denying Patent Owner's Petition to Reopen Prosecution, or (2) one month after VirnetX's appeal brief would otherwise be due.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 28, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	Control No.: 95/001,949
Victor Larson et al.	)	
	)	Group Art Unit: 3992
U.S. Patent No. 8,051,181	)	
	)	Examiner: Dennis G. Bonshock
Issued: November 1, 2011	)	
	)	Confirmation No.: 4522
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the patent owner certifies that a copy of Patent Owner's Petition for an Extension of Time to File an Appeal Brief was served by first-class mail on October 28, 2013, on counsel for the third-party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 28, 2013

By: / Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001949
Filing Date:	28-Mar-2012
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Filer:	Joseph Edwin Palys./Donna Beckford-Harris
Attorney Docket Number:	41484-80200

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**200**

Electronic Acknowledgement Receipt

EFS ID:	17247006
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Donna Beckford-Harris
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	28-OCT-2013
Filing Date:	28-MAR-2012
Time Stamp:	17:44:23
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$200
RAM confirmation Number	5444
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		Petition_for_Extension_of_Time.pdf	108801 69e8bf345b29cd7be7dbbc9deb96736af3e4579d	yes	6

Multipart Description/PDF files in .zip description

Document Description	Start	End
Reexam Request for Extension of Time	1	5
Reexam Certificate of Service	6	6

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30563 3fd9931edcd9febea3727a01554bbbb97f1f78e3	no	2

Warnings:

Information:

Total Files Size (in bytes):	139364

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 11/15/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	
ART UNIT	PAPER NUMBER
3992	
MAIL DATE	DELIVERY MODE
11/15/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date: MAILED

NOV 15 2013

CENTRAL REEXAMINATION UNIT

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Decision on Petition for Waiver of Timing Requirements in Reexamination	Control Nos.: 95/001,949

1. THIS IS A DECISION ON THE PETITION FILED **October 28, 2013**.

2. THIS DECISION IS ISSUED PURSUANT TO 37 CFR 1.183, requesting waiver of the timing requirements set forth in the following rule(s):

A. □ 37 CFR 1.515(c) – The requester may seek review by a petition to the Director under § 1.181 within one month of the mailing date of the examiner's determination refusing *ex parte* reexamination.
B. □ 37 CFR 41.31 – Any notice of appeal must be filed within the time period provided under § 1.134 for reply.
C. □ 37 CFR 41.37(a)(1) – Appellant must file a brief under this section within two months from the date of filing the notice of appeal under § 41.31.
D. □ 37 CFR 41.41(a)(1) – Appellant may file a reply brief to an examiner's answer within two months from the date of the examiner's answer.
E. ☒ 37 CFR 41.66(a) – An appellant's brief must be filed no later than two months from the latest filing date of the last-filed notice of appeal or, if any party to the proceeding is entitled to file an appeal or cross appeal but fails to timely do so, no later than two months from the expiration of the time for filing (by the last party entitled to do so) such notice of appeal or cross appeal. The time for filing an appellant's brief or an amended appellant's brief may not be extended.
F. □ 37 CFR 41.66(b) – Once an appellant's brief has been properly filed, any brief must be filed by respondent within one month from the date of service of the appellant's brief. The time for filing a respondent's brief or an amended respondent's brief may not be extended.
G. □ 37 CFR 41.66(d) – Any appellant may file a rebuttal brief under § 41.71 within one month of the date of the examiner's answer. The time for filing a rebuttal brief may not be extended.
H. □ 37 CFR 41.71(e) – The one-month period for filing a rebuttal brief in an *inter partes* reexamination proceeding that overcomes all the reasons for non-compliance stated in a prior notification may not be extended.
I. □ Waiver of a timing requirement where the service has been certified to the Office, but not received by the petitioning party (requires factual proof of nonreceipt, absence from party's docket system, and a showing that the docket system is reliable for receipt of reexamination correspondence).
J. □ Other:

The petition is before the Office of Patent Legal Administration for consideration.

3. FORMAL MATTERS
Petitioner requests that the period for taking action be extended until one month after a final decision is made on the July 9, 2013 petition filed under § 1.181.

A. ☒ Petition fee per 37 CFR §1.17(f)):
   i. ☒ Petition includes authorization to debit a deposit account.
   ii. □ Petition includes authorization to charge a credit card account.
   iii. ☒ Other: Petitions in a reexamination proceeding, except for those specifically enumerated in 37 CFR 1.550(i) and 1.937(d) are subject to the fee set forth in 37 C.F.R. 1.20(c); currently $1,940.

B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
C. ☒ Petition was timely filed.
D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)

A. □ Granted or ☒ Granted-in-part for **two months**, because the petition for extension of time was filed to obtain the results of (a decision on) a petition(s) filed on **July 9, 2013.** A decision on the petition(s) has (have) not yet been rendered. In the event requester were to have filed a paper merely to keep the proceeding pending, in this case, that filing would cause an unnecessary expenditure of resources by the Central Reexamination Unit (CRU) to consider a paper that could become moot, should the petition be granted.
Under the current facts and circumstances of the proceeding, an extension of time under 37 C.F.R. § 1.183 is granted to the extent that petitioner's time period is extended to run through a date that is **two months** from the mailing date of this decision.

i. □ The time extension granted above applies to the period running for both parties in the *inter partes* reexamination (*i.e.*, the time for both parties to file a brief).

B. □ Granted to the extent that the date of service is deemed to be ____________, the date of actual receipt by the party. The petitioner has made a sufficient evidentiary showing that the other party's paper, although served, was not received by petitioner, was not marked in petitioner's docketing system, and that petitioner's docketing system was such that any reexamination paper would have been properly docketed by that system.

C. ☒ Other/comment: In the event that less than two weeks before the brief due date remain and the petitions have not been decided, petitioner may file a renewed petition for extension of time. In such a situation, petitioner should contact the undersigned to indicate that such a renewed petition is being filed, in order that the Office may timely address the renewed petition.

D. □ Dismissed because:

i. □ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).

ii. □ The present petition requests rule waiver under § 1.183 to extend the time until the Office issues a decision on the party's petition(s) filed on____________. That petition was dismissed in an Office decision issued on ______________. The extension was sought for the purposes of (1) preventing unnecessary expenditure of Patent Office resources, (2) promoting the interests of justice, and (3) to resolve issues that may result in a redundant/wasted briefing or other Office consideration. In view of the dismissal of the petition, questions of unnecessary expenditure of resources and redundant briefing or Office consideration are now moot. In view of the statutory requirement that the Office handle proceedings with "special dispatch," petitioner has failed to show the existence of an extraordinary situation for which justice requires relief in the form of extension of time to file an appellant's brief.
Therefore, the instant petition is **dismissed** to the extent that the requested extension is not granted. However, in view of the circumstances of the present proceeding, the time to take action is extended to run through a date that is two weeks from the mailing date of this decision.

iii. □ The time extension granted above applies to the period running for both parties in the *inter partes* reexamination (*i.e.*, the time for both parties to file a brief).

iv. □ Other/comment: ____.

5. CONCLUSION

Telephone inquiries with regard to this decision should be directed to the undersigned at **571-272-7700**, or to Mark Reinhart, Reexamination Specialist, at **571-272-1611**.

/ Michael Cygan /	**Senior Legal Advisor**	**November 15, 2013**
[*Signature*]	(Title)	(Date)

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U.S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE
COMMUNICATION LINK BETWEEN
COMPUTERS OF VIRTUAL PRIVATE
NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S RENEWED PETITION FOR AN EXTENSION OF TIME TO FILE AN APPEAL BRIEF

VirnetX Inc., the owner of U.S. Patent No. 8,051,181 ("the '181 patent"), files this renewed petition under 37 C.F.R. § 1.183 and M.P.E.P. § 2673.02, and requests that the Director waive or suspend the requirements of 37 C.F.R. § 41.66(a), prohibiting an extension of time for filing an appeal brief. The Office previously waived this prohibition and granted an extension of time for VirnetX to file its appeal brief because VirnetX's Petition Seeking Review of Decision Denying Patent Owner's Petition to Reopen Prosecution ("Petition Seeking Review") remains pending. A favorable decision on the Petition Seeking Review would eliminate the need for filing an appeal brief, and the extension would avoid unnecessarily burdening the Office and the parties with preparing, filing, and processing appeal briefs that may become moot if the Office reopens prosecution and the rejections are altered or withdrawn.

In the prior decision granting the extension of time, the Office stated, "[i]n the event that less than two weeks before the brief due date remain and the petitions have not been decided, petitioner may file a renewed petition for extension of time." (11/15/13 Decision on Petition for Waiver of Timing Requirements in Reexamination at 2.) The Office also stated that "petitioner should contact the undersigned to indicate that such a renewed petition is being filed, in order that the Office may timely address the renewed petition." (*Id.*) Consistent with the Office's guidance in the 11/15/13 Decision, and because the Petition Seeking Review remains pending, VirnetX renews its request for an extension of time to file its appeal brief.

To the extent entry and consideration of this renewed petition requires suspension of any rules in addition to 37 C.F.R. § 41.66(a), VirnetX requests suspension under 37 C.F.R. § 1.183. Please charge any fee due in connection with the filing of this Petition to Deposit Account No. 06-0916.

I. BACKGROUND

Third-party requester Apple Inc. ("Apple") filed a Request for Reexamination ("Request" or "Req.") on March 28, 2012. The Office granted the Request and issued a first Office Action on June 4, 2012, incorporating by reference nearly all of the Request. VirnetX filed a response ("Response") to the first Office Action on September 4, 2012. Apple filed third-party comments ("Comments") to VirnetX's Response on October 22, 2012. The Office subsequently issued an Action Closing Prosecution ("ACP") on January 16, 2013.

On March 18, 2013, VirnetX petitioned the Office to reopen prosecution. In the Petition, VirnetX explained that the ACP provided new bases for its rejections by, among other things, relying on different features in the references that were not previously relied upon in the initial Office Action. (Petition 2-7.) The Office denied VirnetX's Petition in a May 28, 2013, decision. VirnetX petitioned for review on July 9, 2013. The Director has not yet rendered a decision on this Petition Seeking Review. Nonetheless, the Office issued a Right of Appeal Notice ("RAN") on August 16, 2013, and VirnetX filed a Notice of Appeal on September 16, 2013. Based on the pendency of the Petition Seeking Review, on November 15, 2013, the Office granted VirnetX an extension of time to file its appeal brief and noted that VirnetX may renew its extension request if the Petition Seeking Review remains pending. Consistent with the Office's guidance, because the Petition Seeking Review remains pending, VirnetX now files this renewed Petition.

II. ARGUMENT

VirnetX renews its request for an extension of time because a decision by the Director on VirnetX's Petition Seeking Review may result in reopening prosecution, which would avoid the need to file an appeal brief. The extension would therefore conserve the resources of the Office, Requester, and VirnetX.

Granting an extension is also consistent with the procedure set forth in M.P.E.P. § 2673.02, which recommends seeking waiver of the prohibition of an extension of time to file an appeal brief while awaiting a decision on a petition to enter an amendment into the record. This case is analogous to the situation contemplated by the M.P.E.P. because, in both scenarios, the Director's decision could significantly alter the scope and content of any appeal. In the § 2673.02 scenario, the amendment could alter the scope of the claims. Similarly, reopening prosecution in this case could result in introduction of further evidence to rebut the Office's rejections, as detailed in the Petition Seeking Review. It may also result in the Examiner withdrawing previously maintained rejections. Thus, VirnetX's request is consistent with the procedure outlined in § 2673.02.

An extension here is also consistent with prior Office decisions addressing similar circumstances. For example, the Office granted VirnetX an extension of time to obtain the results of pending petitions to reopen prosecution and to enter an expert declaration into the record. (*See* Control No. 95/001,851, Decision on Petition for Waiver of Timing Requirements in Reexamination at 2 (Nov. 20, 2013).) The extension decision noted that, in the event VirnetX "were to have filed a paper merely to keep the proceeding pending, in this case, that filing would cause unnecessary expenditure of resources by the Central Reexamination Unit (CRU) to consider a paper that could become moot, should the petition be granted." (*Id.*) There, the Office ultimately granted VirnetX's petition to reopen prosecution and entered the expert declaration, and the extension of time served its purpose of avoiding burdening the Office and the parties with unnecessary filings.[1] The same reasoning applies here, as requiring briefing to proceed before the Director decides the Petition Seeking Review would not only result in an unnecessary expenditure of resources regarding VirnetX's appeal brief, but would also trigger deadlines for other briefs, such as Apple's respondent brief. Without the extension, the Office may unnecessarily need to expend resources on multiple papers that could become moot.

To avoid the need for continued petition practice, VirnetX proposes that it would be most efficient to extend the time for filing its appeal brief until one month after the Director decides VirnetX's Petition Seeking Review. If the Office prefers not to link the appeal-brief deadline to

[1] The Office similarly reopened prosecution in Control No. 95/001,856, which also involves a VirnetX patent. However, the Office declined to reopen prosecution regarding the VirnetX patents involved in Control Nos. 95/001,788 and 95/001,789. Those cases present the identical issue that the Office found to warrant reopening prosecution in 95/001,851 and 95/001,856, so on December 20, 2013, VirnetX petitioned for reconsideration of the decision not to reopen prosecution.

the decision date of this other petition, VirnetX alternatively requests a one-month extension of time after VirnetX's appeal brief would otherwise be due. This would most efficiently conserve the resources of the Office, Requester, and VirnetX, particularly considering the many concurrent proceedings requiring attention from VirnetX and the Office.[2]

III. CONCLUSION

For these reasons, VirnetX requests that the Director suspend the requirements of 37 C.F.R. § 41.66(a), which prohibits an extension of time for filing an appeal brief. VirnetX also renews its request that the Director grant an extension of time for filing its appeal brief until one month after the Director decides VirnetX's Petition Seeking Review, or alternatively, one month after VirnetX's appeal brief would otherwise be due.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 2, 2014

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

[2] VirnetX is also currently involved in the following 10 related reexamination proceedings: Control Nos. 95/001,679 and 95/001,682 involving U.S. Patent No. 6,502,135; Control Nos. 95/001,697 and 95/001,714 involving U.S. Patent No. 7,490,151; Control No. 95/001,746 involving U.S. Patent No. 6,839,759; Control Nos. 95/001,788 and 95/001,851 involving U.S. Patent No. 7,418,504; Control Nos. 95/001,789 and 95/001,856 involving U.S. Patent No. 7,921,211; and Control No. 95/001,792 involving U.S. Patent No. 7,188,180.

VirnetX is additionally involved in the following nine related *inter partes* review proceedings: IPR2014-00171 and -00172 involving U.S. Patent No. 6,502,135; IPR2014-00173 involving U.S. Patent No. 7,490,151; IPR2014-00174 and -00175 involving U.S. Patent No. 7,921,211; IPR2014-00176 and -00177 involving U.S. Patent No. 7,418,504; and IPR2014-00237 and -00238 involving U.S. Patent No. 8,504,697.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.

U.S. Patent No. 8,051,181

Issued: November 1, 2011

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Control No.: 95/001,949

Group Art Unit: 3992

Examiner: Dennis G. Bonshock

Confirmation No.: 4522

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the patent owner certifies that a copy of Patent Owner's Renewed Petition for an Extension of Time to File an Appeal Brief was served by first-class mail on January 2, 2014, on counsel for the third-party requester at the following address:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 2, 2014

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	17797237
Application Number:	95001949
International Application Number:	
Confirmation Number:	4522
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	8051181
Customer Number:	22852
Filer:	Joseph Edwin Palys./Virginia McNelis-Clark
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	41484-80200
Receipt Date:	02-JAN-2014
Filing Date:	28-MAR-2012
Time Stamp:	12:04:53
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Petition.pdf	106539 252fd5f6abf4a7f1e333cbbf0fc3491c54e27a2c	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Petition for review by the Office of Petitions.	1	5
	Reexam Certificate of Service	6	6
Warnings:			
Information:			
	Total Files Size (in bytes):	106539	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,949	03/28/2012	8051181	41484-80200	4522

22852 7590 01/14/2014
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
BONSHOCK, DENNIS G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
01/14/2014	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

Date:

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001949
PATENT NO. : 8051181
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Decision on Petition for Waiver of Timing Requirements in Reexamination	Control Nos.: 95/001,949

1. THIS IS A DECISION ON THE PETITION FILED **January 2, 2014**.

2. THIS DECISION IS ISSUED PURSUANT TO 37 CFR 1.183, requesting waiver of the timing requirements set forth in the following rule(s):

A. □ 37 CFR 1.515(c) – The requester may seek review by a petition to the Director under § 1.181 within one month of the mailing date of the examiner's determination refusing *ex parte* reexamination.
B. □ 37 CFR 41.31 – Any notice of appeal must be filed within the time period provided under § 1.134 for reply.
C. □ 37 CFR 41.37(a)(1) – Appellant must file a brief under this section within two months from the date of filing the notice of appeal under § 41.31.
D. □ 37 CFR 41.41(a)(1) – Appellant may file a reply brief to an examiner's answer within two months from the date of the examiner's answer.
E. ☒ 37 CFR 41.66(a) – An appellant's brief must be filed no later than two months from the latest filing date of the last-filed notice of appeal or, if any party to the proceeding is entitled to file an appeal or cross appeal but fails to timely do so, no later than two months from the expiration of the time for filing (by the last party entitled to do so) such notice of appeal or cross appeal. The time for filing an appellant's brief or an amended appellant's brief may not be extended.
F. □ 37 CFR 41.66(b) – Once an appellant's brief has been properly filed, any brief must be filed by respondent within one month from the date of service of the appellant's brief. The time for filing a respondent's brief or an amended respondent's brief may not be extended.
G. □ 37 CFR 41.66(d) – Any appellant may file a rebuttal brief under § 41.71 within one month of the date of the examiner's answer. The time for filing a rebuttal brief may not be extended.
H. □ 37 CFR 41.71(e) – The one-month period for filing a rebuttal brief in an *inter partes* reexamination proceeding that overcomes all the reasons for non-compliance stated in a prior notification may not be extended.
I. □ Waiver of a timing requirement where the service has been certified to the Office, but not received by the petitioning party (requires factual proof of nonreceipt, absence from party's docket system, and a showing that the docket system is reliable for receipt of reexamination correspondence).
J. □ Other:_.

The petition is before the Office of Patent Legal Administration for consideration.

3. FORMAL MATTERS
Petitioner requests that the period for taking action be extended for one month after the appeal brief would otherwise be due.

A. ☒ Petition fee per 37 CFR §1.17(f)):
  i. ☒ Petition includes authorization to debit a deposit account.
  ii. □ Petition includes authorization to charge a credit card account.
  iii. □ Other: _.
B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
C. ☒ Petition was timely filed.
D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)

A. ☒ Granted or □ Granted-in-part for **two months**, because the petition for extension of time was filed to obtain the results of (a decision on) a petition(s) filed on **July 9, 2013.** A decision on the petition(s) has (have) not yet been rendered. In the event requester were to have filed a paper merely to keep the proceeding pending, in this case, that filing would cause an unnecessary expenditure of resources by the Central Reexamination Unit (CRU) to consider a paper that could become moot, should the petition be granted.
Under the current facts and circumstances of the proceeding, an extension of time under 37 C.F.R. § 1.183 is granted to the extent that petitioner's time period is extended to run through a date that is **two months** from the mailing date of this decision.

i. □ The time extension granted above applies to the period running for both parties in the *inter partes* reexamination (*i.e.*, the time for both parties to file a brief).

B. □ Granted to the extent that the date of service is deemed to be ______________, the date of actual receipt by the party. The petitioner has made a sufficient evidentiary showing that the other party's paper, although served, was not received by petitioner, was not marked in petitioner's docketing system, and that petitioner's docketing system was such that any reexamination paper would have been properly docketed by that system.

C. ☒ Other/comment: The determination of whether "justice requires" further waiver of the rules takes into consideration the delay due to that waiver. In view of the statutory mandate for the Office to handle *inter partes* reexamination proceedings with special dispatch, and in view of the previous extension of time granted on November 15, 2013, and the fact that patent owner is seeking relief on grounds that have been previously dismissed in the May 28, 2013 decision, any future requests for extension of time should not be assumed. The grant of the instant decision is tailored to that necessary to prevent waste of resources from a filed brief that would be moot in view of a granted petition. Such relief is not for extra time for preparing briefing following the decision on the petition filed on July 9, 2013.

D. □ Dismissed because:

i. □ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).

ii. □ The present petition requests rule waiver under § 1.183 to extend the time until the Office issues a decision on the party's petition(s) filed on______________. That petition was dismissed in an Office decision issued on ______________. The extension was sought for the purposes of (1) preventing unnecessary expenditure of Patent Office resources, (2) promoting the interests of justice, and (3) to resolve issues that may result in a redundant/wasted briefing or other Office consideration. In view of the dismissal of the petition, questions of unnecessary expenditure of resources and redundant briefing or Office consideration are now moot. In view of the statutory requirement that the Office handle proceedings with "special dispatch," petitioner has failed to show the existence of an extraordinary situation for which justice requires relief in the form of extension of time to file an appellant's brief.
Therefore, the instant petition is **dismissed** to the extent that the requested extension is not granted. However, in view of the circumstances of the present proceeding, the time to take action is extended to run through a date that is two weeks from the mailing date of this decision.

iii. □ The time extension granted above applies to the period running for both parties in the *inter partes* reexamination (*i.e.*, the time for both parties to file a brief).

iv. □ Other/comment: ____.

5. CONCLUSION

Telephone inquiries with regard to this decision should be directed to the undersigned at **571-272-7700**, or to Mark Reinhart, Reexamination Specialist, at 571-272-1611.

/ Michael Cygan /	**Senior Legal Advisor**	**January 13, 2014**
[*Signature*]	(Title)	(Date)