

DEC 23 2013

FINNEGAN

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
WWW.FINNEGAN.COM

FACSIMILE TRANSMITTAL

TO

Name:
Company: USPTO
Fax Number: 571-273-8300
Phone Number:
Date: December 23, 2013
Subject: Notice of Hearing

FROM

Name: Joe Palys
Phone Number: 571-203-2713
Fax Number Verified by: S. Hardy MD-717
Total Pages (including cover): 3
Our File No.: 11798.0005-00

Confirmation Copy to Follow: N

MESSAGE

Please see the attached.

If there is a problem with this transmission, notify the sender at the number above.

This facsimile is intended only for the individual to whom it is addressed and may contain information that is privileged, confidential, or exempt from disclosure under applicable law. If you have received this facsimile in error, please notify the sender immediately by telephone (collect), and return the original message by first-class mail to the address below.

901 NEW YORK AVENUE, NW | WASHINGTON, DC 20001-4413
PHONE: 202.408.4000 | FAX: 202.408.4400

RECEIVED
CENTRAL FAX CENTER

DEC 23 2013

Page 1



FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

Appeal No:
Appellant:
Inter Partes Reexamination No:
Hearing Room:
Hearing Docket:
Hearing Date:
Hearing Time:
Location:

2014-000591
VIRNETX INC. (OWNER)
95/001,792
B
A
Wednesday, February 26, 2014
01:00 PM
Madison Building - East Wing
600 Dulany Street, 9th Floor
Alexandria, Virginia 22313-1450

**NOTICE OF HEARING
CONFIRMATION REQUIRED WITHIN TWENTY-ONE DAYS**

Your attention is directed to 37 CFR § 41.73. The above identified appeal will be heard by the Patent Trial and Appeal Board on the date indicated. Hearings will commence at the time set and as soon as the argument in one appeal is concluded, the succeeding appeal will be taken up. The time allowed for argument is thirty minutes for each appellant or respondent who has requested an oral hearing, unless additional time is requested and permitted before the argument is commenced. Pursuant to § 41.73(d), if any other party to the appeal desires to participate in the oral hearing, but has not yet requested an oral hearing, a request for oral hearing and the fee set forth in § 41.20(b)(3) must be filed within the time period set in this Notice. No appellant or respondent will be permitted to participate in an oral hearing unless he or she has requested an oral hearing and submitted the fee set forth in § 41.20(b)(3). If there are any inquiries, please contact the Clerk of the Board at 571-272-9797.

The reexamination involved in this appeal is open to the public. Accordingly, the hearing in this appeal is open to the public.

CONFIRMATION OR WAIVER OF THE HEARING IS REQUIRED. This form must be completed below and facsimile transmitted to both: (1) the USPTO Central fax number (official copy), and (2) the Patent Trial and Appeal Board fax number (courtesy copy) within TWENTY-ONE (21) DAYS from the mailing date of this notice indicating confirmation or waiver of the hearing. A copy of this notice may be alternately filed by mail if facsimile is not available.

PTAB HEARINGS FAX No: (571) 273-9797

USPTO Central Fax No: (571) 273-8300

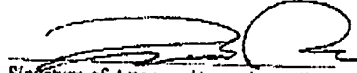
PTAB Mailing Address: Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. BOX 1450
Alexandria, Virginia 22313-1450

In all communications relating to this appeal, please identify the appeal by its number.

Page 2

CHECK ONE: HEARING ATTENDANCE CONFIRMED () HEARING ATTENDANCE WAIVED

[] A request for oral hearing and the fee set forth in § 41.20(b)(3) is attached to this Hearing Confirmation.

	12/23/13	46,508
Signature of Attorney/Agent/Appellant	Date	Registration No.

Names of other visitors expected to accompany counsel:

Naveen Modi

James Stein

Sameer Mathur

For information on visitor access to hearing rooms and security procedures at the USPTO Alexandria Campus, see http://www.uspto.gov/web/offices/dcmi/cesame/qa/visitor.html#all_events

cc: Third Party Requester

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE , SUITE 700
DALLAS, TX 75219

RECEIVED
CENTRAL FAX CENTER

DEC 16 2013

haynesboone

Haynes and Boone, LLP
Attorneys and Counselors
2505 N Plano Road, Suite 4000
Richardson, Texas 75082-4101
Phone: (972) 680-7550
Fax: (972) 680-7551
www.haynesboone.com

Date: Monday, December 16, 2013 1:28:44 PM

Total Pages Including Cover: 03

To: USPTO Central Fax

Company: U. S. Patent and Trademark Off

Fax: 15712738300

Telephone:

Client/Matter: 43614. 100

From: O'Connor, Theresa

Direct Telephone: 972-739-8644

Direct Fax: 972-692-9106

Should you have any problem with this transmission, please call: 972-739-8644

Message:

Confidentiality Note: The information contained in this facsimile message is privileged and confidential and is intended only for the use of the addressee. The term "privileged and confidential" includes, without limitation, attorney-client privileged communications, attorney work product, trade secrets, and any other proprietary information. Nothing in this facsimile is intended by the attorney or the client to constitute a waiver of the confidentiality of this message. If the reader of this message is not the intended recipient, or employee/agent of the intended recipient, you are hereby notified that any duplication, or distribution of this communication is unauthorized. If you have received this message in error, please notify us by telephone immediately so that we can arrange for the return of the original documents to us at no cost to you.

RECEIVED
CENTRAL FAX CENTER

DEC 16 2013

Page 1



HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

Appeal No: 2014-000,591
Appellant: HAYNES AND BOONE, LLP (3RD.PTY.REQ)
Inter Partes Reexamination No: 95/001,792
Hearing Room: B
Hearing Docket: A
Hearing Date: Wednesday, February 26, 2014
Hearing Time: 01:00 PM
Location: Madison Building - East Wing
600 Dulany Street, 9th Floor
Alexandria, Virginia 22313-1450

**NOTICE OF HEARING
CONFIRMATION REQUIRED WITHIN TWENTY-ONE DAYS**

Your attention is directed to 37 CFR § 41.73. The above identified appeal will be heard by the Patent Trial and Appeal Board on the date indicated. Hearings will commence at the time set and as soon as the argument in one appeal is concluded, the succeeding appeal will be taken up. The time allowed for argument is thirty minutes for each appellant or respondent who has requested an oral hearing, unless additional time is requested and permitted before the argument is commenced. Pursuant to § 41.73(d), if any other party to the appeal desires to participate in the oral hearing, but has not yet requested an oral hearing, a request for oral hearing and the fee set forth in § 41.20(b)(3) must be filed within the time period set in this Notice. No appellant or respondent will be permitted to participate in an oral hearing unless he or she has requested an oral hearing and submitted the fee set forth in § 41.20(b)(3). If there are any inquiries, please contact the Clerk of the Board at 571-272-9797.

The reexamination involved in this appeal is open to the public. Accordingly, the hearing in this appeal is open to the public.

CONFIRMATION OR WAIVER OF THE HEARING IS REQUIRED. This form must be completed below and facsimile transmitted to both: (1) the USPTO Central fax number (official copy), and (2) the Patent Trial and Appeal Board fax number (courtesy copy) within TWENTY-ONE (21) DAYS from the mailing date of this notice indicating confirmation or waiver of the hearing. A copy of this notice may be alternately filed by mail if facsimile is not available.

PTAB HEARINGS FAX No: (571) 273-9797


USPTO Central Fax No: (571) 273-8300

PTAB Mailing Address: Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. BOX 1450
Alexandria, Virginia 22313-1450

In all communications relating to this appeal, please identify the appeal by its number.

CHECK ONE: HEARING ATTENDANCE CONFIRMED HEARING ATTENDANCE WAIVED

A request for oral hearing and the fee set forth in § 41.20(b)(3) is attached to this Hearing Confirmation.

 12/16/14 50271
Signature of Attorney/Agent/Appellant Date Registration No.

Names of other visitors expected to accompany counsel:

David McCombs, Theodore Foster

John Desmarais, Karim Oussayef

For information on visitor access to hearing rooms and security procedures at the USPTO Alexandria Campus, see http://www.uspto.gov/web/offices/dca/m/counsel/contact.htm#bna_contacts

cc: Patent Owner

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
901 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20001-4413



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes details for application 95/001,792, inventor FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP, and examiner HUGHES, DEANDRA M.

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.

The United States Patent and Trademark Office
PATENT TRIAL AND APPEAL BOARD



FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER,LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

Appeal No: 2014-000591
Appellant: VIRNETX INC. (OWNER)
Inter Partes Reexamination No: 95/001,792
Hearing Room: B
Hearing Docket: A
Hearing Date: Wednesday, February 26, 2014
Hearing Time: 01:00 PM
Location: Madison Building - East Wing
600 Dulany Street, 9th Floor
Alexandria, Virginia 22313-1450

**NOTICE OF HEARING
CONFIRMATION REQUIRED WITHIN TWENTY-ONE DAYS**

Your attention is directed to 37 CFR § 41.73. The above identified appeal will be heard by the Patent Trial and Appeal Board on the date indicated. Hearings will commence at the time set and as soon as the argument in one appeal is concluded, the succeeding appeal will be taken up. The time allowed for argument is thirty minutes for each appellant or respondent who has requested an oral hearing, unless additional time is requested and permitted before the argument is commenced. Pursuant to § 41.73(d), if any other party to the appeal desires to participate in the oral hearing, but has not yet requested an oral hearing, a request for oral hearing and the fee set forth in § 41.20(b)(3) must be filed within the time period set in this Notice. No appellant or respondent will be permitted to participate in an oral hearing unless he or she has requested an oral hearing and submitted the fee set forth in § 41.20(b)(3). If there are any inquiries, please contact the Clerk of the Board at 571-272-9797.

The reexamination involved in this appeal is open to the public. Accordingly, the hearing in this appeal is open to the public.

CONFIRMATION OR WAIVER OF THE HEARING IS REQUIRED. This form must be completed below and facsimile transmitted to both: (1) the USPTO Central fax number (official copy), and (2) the Patent Trial and Appeal Board fax number (courtesy copy) within TWENTY-ONE (21) DAYS from the mailing date of this notice indicating confirmation or waiver of the hearing. A copy of this notice may be alternately filed by mail if facsimile is not available.

PTAB HEARINGS FAX No: (571) 273-9797

USPTO Central Fax No: (571) 273-8300

PTAB Mailing Address: Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. BOX 1450
Alexandria, Virginia 22313-1450

In all communications relating to this appeal, please identify the appeal by its number.

CHECK ONE: () HEARING ATTENDANCE CONFIRMED () HEARING ATTENDANCE WAIVED

[] A request for oral hearing and the fee set forth in § 41.20(b)(3) is attached to this Hearing Confirmation.

Signature of Attorney/Agent/Appellant Date Registration No.

Names of other visitors expected to accompany counsel:

For information on visitor access to hearing rooms and security procedures at the USPTO Alexandria Campus, see http://www.uspto.gov/web/offices/dcom/gcounsel/contact.htm#bpai_contacts

cc: Third Party Requester

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE , SUITE 700
DALLAS, TX 75219



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 95/001,792, 10/25/2011, 7,188,180, 43614.100, 1972
Row 2: 22852, 7590, 12/05/2013, FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP, 901 NEW YORK AVENUE, NW, WASHINGTON, DC 20001-4413, EXAMINER HUGHES, DEANDRA M, ART UNIT 3992, PAPER NUMBER, MAIL DATE 12/05/2013, DELIVERY MODE 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.

The United States Patent and Trademark Office
PATENT TRIAL AND APPEAL BOARD



HAYNES AND BOONE, LLP	Appeal No:	2014-000,591
IP SECTION	Appellant:	HAYNES AND BOONE, LLP (3RD.PTY.REQ)
2323 VICTORY AVENUE	Inter Partes Reexamination No:	95/001,792
SUITE 700	Hearing Room:	B
DALLAS, TX 75219	Hearing Docket:	A
	Hearing Date:	Wednesday, February 26, 2014
	Hearing Time:	01:00 PM
	Location:	Madison Building - East Wing 600 Dulany Street, 9th Floor Alexandria, Virginia 22313-1450

**NOTICE OF HEARING
CONFIRMATION REQUIRED WITHIN TWENTY-ONE DAYS**

Your attention is directed to 37 CFR § 41.73. The above identified appeal will be heard by the Patent Trial and Appeal Board on the date indicated. Hearings will commence at the time set and as soon as the argument in one appeal is concluded, the succeeding appeal will be taken up. The time allowed for argument is thirty minutes for each appellant or respondent who has requested an oral hearing, unless additional time is requested and permitted before the argument is commenced. Pursuant to § 41.73(d), if any other party to the appeal desires to participate in the oral hearing, but has not yet requested an oral hearing, a request for oral hearing and the fee set forth in § 41.20(b)(3) must be filed within the time period set in this Notice. No appellant or respondent will be permitted to participate in an oral hearing unless he or she has requested an oral hearing and submitted the fee set forth in § 41.20(b)(3). If there are any inquiries, please contact the Clerk of the Board at 571-272-9797.

The reexamination involved in this appeal is open to the public. Accordingly, the hearing in this appeal is open to the public.

CONFIRMATION OR WAIVER OF THE HEARING IS REQUIRED. This form must be completed below and facsimile transmitted to both: (1) the USPTO Central fax number (official copy), and (2) the Patent Trial and Appeal Board fax number (courtesy copy) within TWENTY-ONE (21) DAYS from the mailing date of this notice indicating confirmation or waiver of the hearing. A copy of this notice may be alternately filed by mail if facsimile is not available.

PTAB HEARINGS FAX No: (571) 273-9797

USPTO Central Fax No: (571) 273-8300

PTAB Mailing Address: Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. BOX 1450
Alexandria, Virginia 22313-1450

In all communications relating to this appeal, please identify the appeal by its number.

CHECK ONE: () HEARING ATTENDANCE CONFIRMED () HEARING ATTENDANCE WAIVED

[] A request for oral hearing and the fee set forth in § 41.20(b)(3) is attached to this Hearing Confirmation.

Signature of Attorney/Agent/Appellant Date Registration No.

Names of other visitors expected to accompany counsel:

For information on visitor access to hearing rooms and security procedures at the USPTO Alexandria Campus, see http://www.uspto.gov/web/offices/dcom/gcounsel/contact.htm#bpai_contacts

cc: Patent Owner

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
901 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20001-4413



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes fields for EXAMINER (HUGHES, DEANDRA M), ART UNIT (3992), PAPER NUMBER, MAIL DATE (10/25/2013), and DELIVERY MODE (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

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

FINNEGAN,
HENDERSON,
FARABOW, GARRETT
& DUNNER LLP
901 NEW YORK
AVENUE, NW
WASHINGTON, DC
20001-4413

Appeal No: 2014-
000591
Inter Partes
Reexamination
Control No: 95/001,792
Appellant: 7,188,180 et
al.

Patent Trial and Appeal Board Docketing Notice

Inter Partes Reexamination Control No. 95/001,792 was received from the Technology Center at the Board on October 22, 2013 and has been assigned Appeal No: 2014-000591.

In all future communications regarding this appeal, please include both the *Inter Partes* Reexamination Control Number and the appeal number.

The mailing address for the Board is:

PATENT TRIAL and APPEAL BOARD
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VIRGINIA 22313-1450

Telephone inquiries can be made by calling 571-272-9797 and referencing the appeal number listed above.

By order of the Patent Trial and Appeal Board.

JAG

cc: Third Party Requester

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE , SUITE 700
DALLAS, TX 75219

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor Larson et al.) Control No.: 95/001,792
)
U.S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

REQUEST FOR ORAL HEARING

Pursuant to 37 C.F.R. § 41.73(b), VirnetX Inc., the owner of U.S. Patent No. 7,188,180, requests an oral hearing. This request is timely since it is made within two months after the mailing date of the Examiner's Answer. The fee of \$1,300.00 required by 37 C.F.R. § 41.20(b)(3) is being submitted concurrently with the filing of this request.

Please grant any extension of time and charge any additional fees to Deposit Account No. 06-0916.

Respectfully submitted,
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 10, 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.: 95/001,792
)
U.S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK)

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 Request for Oral Hearing was served by first-class mail on October 10, 2013 on counsel for the third party Requester at the following address:

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: October 10, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	Joseph Edwin Palys./Sheryl Lewis				
Attorney Docket Number:	43614.100				
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:					
Request for Oral Hearing	1403	1	1300	1300	
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				1300

Electronic Acknowledgement Receipt

EFS ID:	17090858
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	10-OCT-2013
Filing Date:	25-OCT-2011
Time Stamp:	11:39:04
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1300
RAM confirmation Number	12840
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1		180RequestforOralHearing.pdf	78020 83d6665b7e78efceba54b234036acdc4526567db	yes	2
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Oral Hearing Request-Owner	1	1	
		Reexam Certificate of Service	2	2	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30595 6603a1bcf0a43a91833807b2ad31f3c207a75848	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			108615		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					



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.
-----------------	-------------	----------------------	---------------------	------------------

95/001,792	10/25/2011	7,188,180	43614.100	1972
------------	------------	-----------	-----------	------

22852 7590 09/30/2013
 FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
 LLP
 901 NEW YORK AVENUE, NW
 WASHINGTON, DC 20001-4413

EXAMINER

HUGHES, DEANDRA M

ART UNIT	PAPER NUMBER
----------	--------------

3992

MAIL DATE	DELIVERY MODE
-----------	---------------

09/30/2013

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 <i>Inter Partes</i> Reexamination	Control No.	Patent Under Reexamination	
	95/001,792	7,188,180	
	Examiner	Art Unit	
	DEANDRA HUGHES	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219

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 DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
 Address : COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
95/001,792	25 October, 2011	7,188,180	43614.100

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413	EXAMINER	
	DEANDRA HUGHES	
	ART UNIT	PAPER
	3992	20130918

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

<p>The Examiner's Answer was mailed August 16, 2013.</p> <p>Third Party Requester's Rebuttal Brief was entered on September 13, 2013.</p> <p>No further response by the examiner is appropriate. Any further reply/comments by any party will be not be considered, and may be returned to the party that submitted it. The reexamination proceeding is being forwarded to the Board of Patent Appeals and Interferences for decision on the appeal(s).</p>	
/Deandra M. Hughes/, Reexamination Specialist AU3992	

PTO-90C (Rev.04-03)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of: Victor Larson, et al.	§	Docket No.	43614.100
<i>Inter Partes</i> Reexamination	§		
	§	Examiner:	HUGHES, Deandra
Proceeding No.: 95/001,792	§		
	§	Art Unit:	3992
Patent No.: 7,188,180	§		
	§	Conf. No.	1972
For: Method for establishing secure	§		
communication link between	§		
computers of virtual private network	§		

Mail Stop *Inter Partes* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR ORAL HEARING

The appellant Third Party Requester Cisco Systems, Inc. hereby requests an oral hearing of this appeal. This hearing request is being submitted pursuant to and in accordance with 37 CFR 41.73. The request is timely submitted in response to the Examiner's Answer dated August 16, 2013. A certificate of service is attached herewith. The Commissioner is hereby authorized to charge the fee set forth under 37 CFR 41.20(b)(3), in the amount of \$1300.00. Further, the Commissioner is authorized to charge any additional fees that may be associated with this filing, or credit any overpayment, to the Haynes and Boone, LLP Deposit Account No. 08-1394.

Inter Partes Reexamination
Control No. 95/001,792

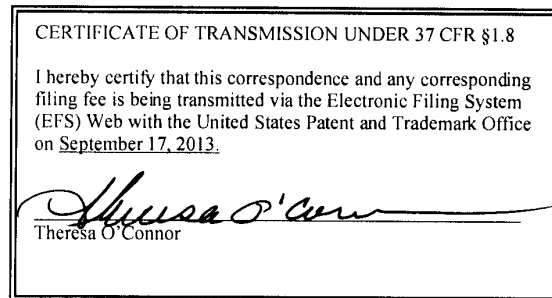
Request for Oral Hearing
By Third Party Requester

Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: September 17, 2013
HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: 972/739-8636
Facsimile: 214/200-0853
Attorney Docket No.: 43614.100



Inter Partes Reexamination
Control No. 95/001,792

Request for Oral Hearing
By Third Party Requester

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the REQUEST FOR ORAL HEARING was served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

the attorneys of record for the assignee of USP 7,188,180 in accordance with 37 CFR § 1.903, on
September 17, 2013.

/David L. McCombs /

David L. McCombs,
Registration No. 32,271

R-343834_1

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:					
Request for Oral Hearing	1403	1	1300	1300	
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				1300

Electronic Acknowledgement Receipt

EFS ID:	16875407
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	17-SEP-2013
Filing Date:	25-OCT-2011
Time Stamp:	14:43:26
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1300
RAM confirmation Number	1115
Deposit Account	081394
Authorized User	MCCOMBS, DAVID L

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		Request_for_Oral_Hearing.pdf	61915 44a49e7b221dc6b8187cdd5646e6669642a2661b	yes	3
Multipart Description/PDF files in .zip description					
	Document Description	Start	End		
	Oral Hearing Request - Third Party Requester	1	2		
	Reexam Certificate of Service	3	3		

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30645 80e8fd2a1d5708fbdacf386b7225261e42e2e34a	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes): 92560

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

Application of: Victor Larson, et al.	§	Docket No.	43614.100
<i>Inter Partes</i> Reexamination	§	Examiner:	HUGHES, Deandra
Patent No. 7,188,180	§	Art Unit:	3992
Proceeding No.: 95/001,792	§	Conf. No.	1972

Mail Stop: *Inter Partes* Reexamination
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

THIRD PARTY REQUESTER CISCO SYSTEMS, INC.'S

REBUTTAL BRIEF

Table of Contents

I.	The Claim Rejections Should Be Reinstated	1
A.	Kiuchi Teaches a “Virtual Private Network Communication Link”	1
B.	Kiuchi Teaches a “Sending an Access Request Message ... Using a Virtual Private Network Communication Link”	2
C.	Kiuchi Anticipates Claim 1 Even Under VirnetX’s Proposed Claim Interpretation of “Virtual Private Network Communication Link”	3
D.	Cisco’s Appeal Does Not Raise a New Ground of Rejection	4
E.	Kiuchi Anticipates Claims 6, 22, and 37	5
F.	Kiuchi Anticipates Claims 8, 24, and 39	7
G.	Kiuchi Anticipates Claims 13, 15, 29, and 31	8
II.	VirnetX Fails to Demonstrate Second Considerations of Non-Obviousness.....	8
1.	VirnetX Fails to Demonstrate Nonobviousness Through Evidence of Secondary Considerations.....	9
2.	The Examiner Properly Rejected VirnetX’s Evidence of Licensing Success	11
III.	Conclusion.....	13
V.	Certificate of Service.....	14

I. The Claim Rejections Should Be Reinstated

The Examiner initially (and correctly) rejected all of the claims subject to reexamination, but then withdrew those rejections. As Third Party Requester Cisco Systems, Inc. showed in its Appeal Brief filed June 28, 2013, Kiuchi and the other prior art references teach the limitations of the claims. The Examiner’s decision to withdraw the rejections was based on the Examiner’s addition of an erroneous and improper narrowing limitation. The Board should reverse the Examiner and reinstate the rejection of all claims subject to reexamination.

This Rebuttal Brief is filed in response to Patent Owner VirnetX, Inc.’s Response Brief (“Resp. Br.”) filed July 29, 2013, and the Examiner’s Answer filed August 16, 2013. Since the Examiner’s Answer simply reiterated her positions from the Right of Appeal Notice, Cisco’s response below focuses on the arguments raised by VirnetX’s Response Brief.

A. Kiuchi Teaches a “Virtual Private Network Communication Link”

This appeal calls for the Board to review the Examiner’s conclusion that claim 1 requires communicating via a *private network*. (RAN at 4.) The Examiner is wrong because she failed to consider all of the words in the claim phrase “virtual private network communication link.” Specifically, the word “virtual” indicates that the privacy of the network may be virtual. For example, encryption can be used to provide privacy to communications over a public network.

The ’180 specification confirms that a virtual private network can exist over a public network. The specification describes, for example, “establishing a secure communication link between a first computer and a second computer over a computer network, *such as the Internet*.” (’180 Patent, 6:42-44, emphasis added.) It further describes “implementing a secure virtual Internet” that “works over the existing Internet infrastructure.” (’180 Patent, 6:22-26.) The specification thus describes secure communication links made over the public Internet, which is not a private network. The Examiner’s claim interpretation improperly excludes such embodiments.

Responding to the Examiner, VirnetX reiterates that “the district court explained that a virtual private network is a ‘network of computers which privately communicate....’” (PO Resp. Br. at 6, emphasis by VirnetX.) However, VirnetX omits the remainder of the court’s construction: “... by encrypting traffic *on insecure communication paths* between the computers.” (Cisco Ex. B-4 at 10.) The court’s construction requires “insecure communication

paths,” which are incompatible with the Examiner’s requirement of a “private network.” The emphasis in the court’s construction is on the privacy of the *communications*, not the privacy of the *network* itself. Accordingly, with a “virtual private network communication link,” privacy is not provided by a private network (as the Examiner erroneously understood). Instead, privacy is provided by a *virtual* private network that “encrypt[s] traffic on insecure communication paths.”

Kiuchi teaches the same kind of *virtual* private network “built on the Internet” as described in the ’180 specification. (Kiuchi at 64.) Specifically, Kiuchi describes the secure connections among computers as forming a “closed HTTP-based virtual network.” (Kiuchi at 69.) Just as in the ’180 specification, the computers in Kiuchi’s closed virtual network communicate over the Internet. They use encryption to provide privacy for their communications. Thus, Kiuchi’s closed HTTP-based virtual network is a “virtual private network,” and the computers participating in Kiuchi’s network—including a client-side proxy and a server-side proxy—communicate via “virtual private network communication links.”

B. Kiuchi Teaches a “Sending an Access Request Message ... Using a Virtual Private Network Communication Link”

VirnetX also argues that Kiuchi lacks sufficient disclosure of “sending an access request message ... using a virtual private network communication link” as recited in claim 1. VirnetX argues that “when a request is sent [in Kiuchi], the proxies have simply begun the lengthy process of working towards establishing a connection to each other.” (Resp. Br. at 4.) Thus, VirnetX reasons, “the client-side proxy has no established ‘link’ to any server-side proxy.” (*Id.*)

VirnetX’s argument is merely an attempt to introduce unrecited limitations into the claim. Specifically, claim 1 does not recite or refer to an *established* link. Thus, VirnetX’s argument is untethered from the claim language and without merit.

VirnetX’s attempted distinction also fails because it is inconsistent with the ’180 specification. The specification describes, for example, “a method for communicating using a private communication link” where the client computer has no established “link” to the server computer. Indeed, the data that is communicated is “used for forming a virtual private connection” between them:

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.

(’180 Patent, 7:47–8:3.)

Thus, the ’180 specification contemplates “using a private communication link” even in the absence of a formally established “link.” As in the quoted example above, the “private communication link” might be used to exchange data “used for forming a virtual private connection.” (’180 Patent, 7:55–56.)

Kiuchi’s teachings are similar. The initial message sent from a client-side proxy to a server-side proxy is a request to establish a connection. (Kiuchi at 65.) The connection request message is encrypted to ensure privacy, then sent between two computers within Kiuchi’s virtual network. (*Id.*) Accordingly, the connection request message is sent “using a virtual private network communication link” as recited in claim 1.

C. Kiuchi Anticipates Claim 1 Even Under VirnetX’s Proposed Claim Interpretation of “Virtual Private Network Communication Link”

Even under VirnetX’s claim interpretation requiring an *established* a virtual private network communication link, Kiuchi anticipates claim 1. Specifically, Kiuchi teaches that after a client-side proxy and server-side proxy complete the steps for establishing a secure, encrypted connection, the client-side proxy transmits an access request message that requests to access a web page:

6) Sending C-HTTP requests to the server-side proxy (Fig. 2g)

Once the connection is established, a client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format.

(Kiuchi at 66.) Kiuchi illustrates below an example request, as it would be dispatched by the client-side proxy, to obtain a web page “sample.html” from the server “server.in.current.connection”:

```
(2)
GET "http://server.in.current.connection/
sample.html"
HTTP/1.0<CR><LF>
```

(Kiuchi at 66.) The request to access a web page is an “access request message.” Since such a request is sent “[o]nce the connection is established” and “in encrypted form,” (Kiuchi at 66), the request is sent, under VirnetX’s proffered interpretation, “using a virtual private network communication link.”

VirnetX argues that this teaching in Kiuchi “fails to disclose ‘accessing a secure computer network address’” because “the server-side proxy has already been accessed via a request for connection.” (Resp. Br. at 7.) This argument has no basis in the claim language. Claim 1 does not recite any limitation requiring the “access request message” to be sent before any request for connection, as VirnetX argues. The argument is also irreconcilably inconsistent with VirnetX’s other assertions. For example, VirnetX argues that the “access request message” must be sent through an *established* connection. (See Resp. Br. at 4.) Now VirnetX asserts that the access request message must be sent *before* a request for connection (and thus, *before* the connection is established). VirnetX fails to explain—and Requester cannot find any supporting disclosure in the ’180 specification for—sending two messages such that each message is sent before the other. Accordingly, VirnetX fails to put forward any cogent distinction between the claim language and Kiuchi’s teachings.

D. Cisco’s Appeal Does Not Raise a New Ground of Rejection

VirnetX alleges that Cisco’s appeal brief raises a “new ground of rejection” by identifying the relevant teachings in Kiuchi that show the error in the Examiner’s decision to withdraw the rejections. (Resp. Br. at 6-7.) VirnetX’s position is without merit.

Cisco has not proposed a new ground of rejection. The appealed ground of rejection remains the same as in the originally filed request: anticipation over Kiuchi. Merely citing additional relevant portions of Kiuchi’s teachings—in response to the Examiner’s statements—does not constitute a new ground of rejection. And unlike the cases that VirnetX cites, VirnetX has had multiple opportunities to respond to the teachings of Kiuchi. *See In re Adler*, No. 2012-1610, slip op. at 9 (Fed. Cir. July 18, 2013) (“The ultimate criterion of whether a rejection is considered ‘new’ ... is whether applicants have had fair opportunity to react to the thrust of the rejection.”) (internal citations omitted). Since VirnetX has had multiple opportunities—including its Response Brief—to respond to Kiuchi, the appealed anticipation rejections do not constitute a “new ground.”

Furthermore, this appeal is Cisco’s first and only opportunity to respond to the Examiner’s interpretation of the claim as requiring the “access request message” to transit an already established connection.¹ VirnetX did not raise any such argument in its response to the first Office Action. The interpretation was first introduced into this proceeding when the Examiner adopted it of her own initiative in the Action Closing Prosecution. *See ACP* at 5. VirnetX declined to respond to the ACP, so Cisco was barred from filing Third Party Comments and highlighting the relevant teachings of Kiuchi under the Examiner’s interpretation. In effect, the Examiner’s interpretation put forward a *new ground of allowance*, and Cisco has not had a “fair opportunity to react to the thrust” of the Examiner’s reasoning. *Cf. In re Kronig*, 539 F.2d 1300, 1302 (CCPA 1976). This appeal is Cisco’s first and only opportunity to correct the Examiner’s error. There is no basis for VirnetX’s assertion that the Board is barred from considering the teachings of Kiuchi as a prior art reference.

E. Kiuchi Anticipates Claims 6, 22, and 37

The Examiner withdrew the rejection of claims 6, 22, and 37 because Kiuchi’s version information “is not inserted into a data packet, as claimed, but rather the C-HTTP version is

¹ Cisco notes that this case is readily distinguished from situations where the Examiner’s authority to consider a prior art reference is in question. *Cf. Belkin Int’l, Inc. v. Kappos*, 696 F.3d 1379 (Fed. Cir. 2012) (limiting an Examiner’s ability to consider prior art references with respect to the claims in reexamination). Here, reexamination of claim 1 (among others) was unambiguously ordered based on Kiuchi. *See Decision on Petition* at 17 (Feb. 10, 2012).

transmitted as request-line or a version-line.” (RAN at 9.) But the Examiner failed to realize that the request-line or version-line (containing the C-HTTP version number) is itself inserted into a data packet. Kiuchi details the contents of certain data packets, such as the C-HTTP Response data packet:

```
2. C-HTTP Response
C-HTTP-Version-Line
Plain-Header
CRLF
*General-Header
*Response-Header
*HTTP/1.0-RESPONSE
CRLF
Digital-Signature
```

Kiuchi at 71. Kiuchi further provides an example C-HTTP Response data packet including the version information “C/HTTP-0.7”:

```
f. Response from the server-side proxy, indicating that
the connection is established
C-HTTP/0.7<CR><LF>
Encryption-Algorithm: RSA<CR><LF>
Encrypted-Header-Length: 341<CR><LF>
Signature-Algorithm: RSA<CR><LF>
Signature-Length: 32<CR><LF>
Message-Digest-Algorithm: MD5<CR><LF>
<CR><LF>
*Status: 200 OK<CR><LF>
*Server-Side-Proxy-IP: 130.69.222.222<CR><LF>
*Server-Side-Proxy-Name:
Coordinating.Center.CSCRG<CR><LF>
*Server-Side-Proxy-Port: 8080<CR><LF>
*Client-Side-Proxy-IP: 130.69.111.111<CR><LF>
*Client-Side-Proxy-Name:
University.of.Tokyo.Branch.Hospital<CR><LF>
*User-Agent-IP: 192.168.123.123<CR><LF>
*Connection-ID: 6zdDfldfcZLj8V!<CR><LF>
*Response-Nonce: ef23dc99<CR><LF>
*Response-Data-Exchange-Key: a-3f(*d.bfs.<CR><LF>
<CR><LF>
*36e2bfc5022208ca8c20307f60d15e2e
```

Kiuchi at 74.

Thus, Kiuchi unambiguously teaches that the C-HTTP version information is inserted into a data packet. The Examiner's stated reason for withdrawing the rejection of claim 6 is contrary to Kiuchi's teachings and therefore unsupported.

VirnetX does not defend, or even address, the Examiner's position. Instead, VirnetX

responds by discussing the Examiner’s tacit acknowledgement that Kiuchi’s C-HTTP version information is a “data value representing a predetermined level of service.” (Resp. Br. at 8.) Notably, however, VirnetX does not provide any argument or reasoning that would distinguish Kiuchi’s version information from the claim language. VirnetX does not challenge or disagree with Cisco’s position in any way.

In summary, the Examiner’s decision to withdraw the rejection of claims 6, 22, and 27 was based on an error that neither the Examiner nor VirnetX have attempted to explain or defend. Neither the Examiner nor VirnetX have put forward any other argument that would distinguish the claims from Kiuchi. Accordingly, the Board should reverse the Examiner and reinstate the rejection of claims 6, 22, and 27 as anticipated by Kiuchi.

F. Kiuchi Anticipates Claims 8, 24, and 39

Claim 8 recites in part, “comparing a value in each data packet ... to a moving window of valid values.” Kiuchi teaches that each data packet includes a “Nonce” value and that the Nonce values are incremented with each data packet. (Kiuchi at 73-75.) The Nonce value of each received data packet is checked to confirm that the Nonce value is valid and not a “replay.” (Kiuchi at 65.)

VirnetX acknowledges that Kiuchi teaches that the Nonce values move, but VirnetX alleges that Kiuchi’s range of valid Nonce values does not move. (Resp. Br. at 8.) This argument defies logic. Since the Nonce values change with every data packet, it is readily understood that the range of acceptable Nonce values must also move. Specifically, for Kiuchi’s replay protection to function, every correctly received Nonce value must be removed from the list of acceptable Nonce values so that, if another packet with the same Nonce value is received in the future, that second packet will be rejected.

VirnetX also argues that a Nonce value “could be checked other than [by] comparing it to a ‘moving window of valid values.’” (Resp. Br. at 8.) However, VirnetX fails to offer a single example of how a Nonce value could be checked to ensure it was not a duplicate of a previously-received Nonce value *without performing a comparison*. The claims do not recite any particular method for performing the “comparing.” VirnetX’s approach of checking for duplicate Nonce values teaches “comparing.”

Thus, VirnetX has not identified any distinction between Kiuchi’s checking of Nonce values and the claim limitation of “comparing a value in each data packet ... to a moving

window of valid values.” The Examiner’s decision to withdraw the rejection of claims 8, 24, and 39 should be reversed and the claims again rejected as anticipated by Kiuchi.

G. Kiuchi Anticipates Claims 13, 15, 29, and 31

The Examiner’s only reason for withdrawing the rejection of claims 13, 15, 29 and 31 was that these claims depend from independent claims the Examiner mistakenly found to be distinguishable over Kiuchi. (RAN at 16.)

VirnetX argues that the claims are separately distinguishable over Kiuchi because while Kiuchi teaches performing the recited steps at a *client-side proxy*, these claims require certain steps to be performed by a “client computer.” (Resp. Br. at 8.) VirnetX fails to explain, however, why Kiuchi’s client-side proxy is not a “client computer.” Since Kiuchi’s intended purpose is to “secure communications between a huge number of computers,” it is understood that the client-side proxy is a *computer*. Kiuchi at 68. And as its name suggests, the *client-side proxy* is operable as a *client*. Thus, the client-side proxy is a “client computer.”

Furthermore, VirnetX’s assertion that Kiuchi’s client-side proxy is not a “client computer” is baseless. VirnetX cites nothing from the ’180 specification to support its argument that “client computer” has a special meaning. VirnetX argues that Kiuchi distinguishes between a “user agent” and the “client-side proxy,” but VirnetX fails to explain why the phrasing of a prior art reference should influence the interpretation of the claims under reexamination. Notably, such an approach to claim interpretation is not mentioned in the Federal Circuit’s most recent and comprehensive *en banc* discussion of claim interpretation. *See Philips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005).

Accordingly, the rejection of claims 13, 15, 29 and 31 as anticipated by Kiuchi should be reinstated alongside the rejection of their respective parent claims.

II. VirnetX Fails to Demonstrate Second Considerations of Non-Obviousness

VirnetX argues that even if the anticipation rejections are reinstated—and they should be—the obviousness rejections of claims 7, 11, 23, 27, 38 and 41 should be overcome by its evidence of secondary considerations. VirnetX’s evidence, however, is woefully insufficient to demonstrate non-obviousness.

1. VirnetX Fails to Demonstrate Nonobviousness Through Evidence of Secondary Considerations

VirnetX has presented evidence in the various *inter partes* reexaminations now pending before the Patent Office, and in none of those cases has an Examiner found any merit in VirnetX’s evidence or argument. The evidence submitted in this appeal is similarly insufficient to overcome the obviousness rejections for a variety of reasons.

a) VirnetX Fails to Establish a Long-Felt Need

“Establishing long-felt need requires objective evidence that an art recognized problem existed in the art for a long period of time without solution.” MPEP 716.04. VirnetX cites a declaration by a named inventor describing different government and private equity programs designed to promote science and technology. (Resp. Br. at 9-10.) The affiant, however, is not a disinterested individual who could provide *objective* evidence; rather, he is a named inventor and the Chief Technology Officer and Chief Scientist of the assignee, VirnetX. (See Short Decl., ¶¶1-2.) The affidavit is not “objective evidence” that a “recognized problem existed in the art for a long period of time without solution.” See MPEP 716.04.

VirnetX also alleges that the long-felt need is demonstrated by a government-funded program to research the “Next Generation Internet.” (Resp. Br. at 10.) That program appears to have been principally directed at “high speed networks that are 100-1000 times faster than today’s Internet.” (VirnetX Ex. B-1 at VNET00219319). VirnetX fails to explain how high-speed networking relates in any way to the claims.

VirnetX further alleges that the original assignee, SAIC, spent “85% of its research budget” developing the claimed technology “in the year the inventions claimed in the ’759 patent were developed.” (Resp. Br. at 10.) The only “evidence” cited is the unsubstantiated affidavit of a VirnetX officer, which as noted above, is not objective evidence. And contrary to VirnetX’s assertion, the affidavit states that “SAIC spent *one-third* of its total patent portfolio efforts on our patent portfolio at that time.” (Short Decl. ¶ 7.) Even if the assertion in VirnetX’s brief were supported by reliable evidence, corporate expenditures *in one year* are not indicative of a problem that existed “for a long period of time without solution.” MPEP 716.04(I).

Finally, for VirnetX’s argument to succeed, “the long-felt need must not have been satisfied by another.” MPEP 716.04(I). To the extent that there was any long-felt need for a secure and easy-to-use communication technology, it had already been satisfied by others, like

Kiuchi. VirnetX does not argue that a long-felt need existed for any feature recited in any of the dependent claims rejected as obvious.

In summary, VirnetX fails to show that any long-felt need existed or that any nexus exists between such a long-felt need and the claims rejected as obvious. VirnetX’s assertion of long-felt need fails to rebut the conclusion of obviousness.

b) VirnetX Fails to Establish the Failure of Others

VirnetX alleges that the failure of others is demonstrated by “15 prestigious organizations [who] took part in the ‘Dynamic Coalitions’ research program.” (Resp. Br. at 10.) That program, however, was directed at “security approaches that ensure continued communications when the composition of the coalition changes or the ad hoc area network is attacked.” (VirnetX Ex. B-3 at 1.) VirnetX does not explain how those program goals relate to the claims rejected as obvious. As such, there is no nexus to the claims and the argument fails.

c) VirnetX Fails to Establish Industry Skepticism

VirnetX alleges that the claimed technology was “met with skepticism by those skilled in the art,” but as evidence of this VirnetX relies on the unsubstantiated testimony of a named inventor and VirnetX officer. (Resp. Br. at 11.) VirnetX also cites to a June 1999 article describing a dinner conversation among executives at four start-up companies, but VirnetX does not explain the supposed relevance of this article. The article does not discuss VirnetX or the ’180 claims. Notably, the ’180 patent application had not even been filed in June 1999. VirnetX does not explain why the executives would have been aware of the ’180 claims, let alone have formed a skeptical opinion of them. Thus, VirnetX fails to establish any industry skepticism.

d) VirnetX Fails to Establish Commercial Success

VirnetX alleges that it can show commercial success through its licensing program. (Resp. Br. at 11.) As evidence, VirnetX alleges that SafeNet “entered into a portfolio license ... in July 2002.” A portfolio license established *before the ’180 patent even issued*, however, has no nexus with ’180 patent, let alone the specific claims rejected as obvious. VirnetX also mentions in passing various other licensees to VirnetX’s patent portfolio. But VirnetX provides no evidence that those portfolio licenses were driven by the features recited in the claims rejected as obvious.

Thus, VirnetX fails to show that its licensing activities are evidence of commercial

success, and further fails to show that any commercial success relates to the claimed technology.

e) VirnetX Fails to Establish Praise and Acceptance by Others

As evidence of “praise,” VirnetX alleges that a “study done by CSMG praised the inventions,” but the alleged study is not provided to substantiate this, to explain who paid for the CSMG study, or to explain why CSMG thought the ’180 claims were praise-worthy. VirnetX also alleges that “Jim Rutt at Network Solutions” wanted to invest in its technology. (Resp. Br. At 12.) There is no evidence regarding what aspect of VirnetX’s “technology” allegedly interested Mr. Rutt or how any alleged interest relates to the ’180 patent claims. And again, the only evidence of Mr. Rutt’s alleged interest is in the affidavit of a VirnetX officer.

More generally, allegations of interest by one study and one person are insufficient. Only *widespread* recognition in the art constitutes objective evidence of nonobviousness, not just positive recognition from a few. *See Kloster Speedsteel AB v. Crucible Inc.*, 793 F.2d 1565, 1574 (Fed. Cir. 1986). VirnetX provides no objective evidence of industry-wide praise, nor is there any showing of a nexus between VirnetX’s general “technology” and the features recited in the claims rejected as obvious. VirnetX’s assertion of industry praise is without merit.

2. The Examiner Properly Rejected VirnetX’s Evidence of Licensing Success

VirnetX argues that the Examiner applied an “unreasonable standard” to its evidence of commercial success through licensing. But VirnetX cannot dispute that a portfolio license does not establish commercial success. The Board has previously set forth the evidence needed to support the use of a list of licensees as evidence of secondary considerations: (i) testimony from a licensee as to why the licensee took a license; (ii) whether the taking of the license was a business cost-benefit analysis with regarding to defending an infringement suit, as opposed to the actual merits of the invention; (iii) the number of entities who refused to take a license and why; (iv) the terms of the licenses and whether the licenses were favorable to the licensee; (v) market information indicating the number of products that are sold under licenses and the number of products that are not under license; (vi) the structure and operation of the devices made by the licensees to determine if those products embody the reasons as to why the “invention” is advantageous over the prior, if at all; (vii) whether the licensee took the licenses for reasons substantively related to each and every one of the claims of the ’180 patent; and (viii) a declaration from a representative of any of the licensees attesting to and praising the merits of the claimed invention. *See Ex parte NTP, Inc.*, Appeal 2008-004603, slip op. at 132-34 (BPAI Dec.

22, 2009). Patent Owner has provided none of these and therefore has not carried the burden of demonstrating that its licensing “evidence” has any bearing on nonobviousness.

The need for a thorough review of all the facts relating to a patent license is exemplified by VirnetX’s highly selective presentation of information about its first litigation with Microsoft. VirnetX cites only the jury’s \$100 million damages finding and Microsoft’s subsequent \$200 million settlement payment. But VirnetX notably omits the jury’s finding of willful infringement, which could have *tripled* the damages award to \$300 million and allowed for an award of attorneys’ fees. The \$100 million jury damages finding also omits pre- and post-judgment interest and any potential damages for future infringement. Thus, VirnetX’s suggestion that Microsoft paid a license fee in excess of its litigation damages is baseless. VirnetX also fails to mention that the jury awarded \$34 million in damages for Microsoft’s infringement of the ’180 patent (VirnetX Ex. A-1 at 2), while Microsoft’s \$200 million settlement was for a *portfolio* license. Finally, VirnetX fails to mention that it had recently sued Microsoft *again*, suggesting that Microsoft’s acceptance of a license may have been motivated not by the value of VirnetX’s alleged technology but by a desire (although ultimately fruitless) to simply “buy peace.”

In summary, VirnetX’s alleged evidence of secondary considerations is wholly insufficient and lacks any nexus with the ’180 patent claims. The evidence of secondary considerations should be afforded no weight. Since VirnetX does not contest any of the proposed obviousness rejections on the merits, the Board should reverse the Examiner and reinstate these rejections:

- Claims 11, 27 and 41 are obvious over Kiuchi, and
- Claims 7, 23, and 38 are obvious over Kiuchi in view of Martin.

III. Conclusion

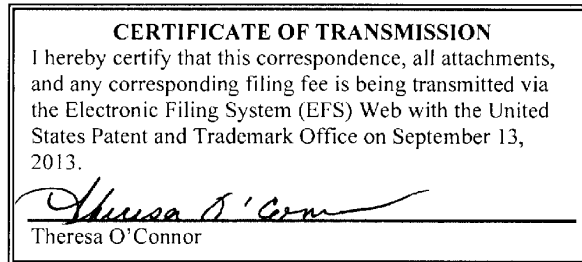
For the reasons provided above, Requester Cisco Systems respectfully asks the Board to reverse the decisions of the Examiner and to reinstate all of the withdrawn claim rejections. The Director is hereby authorized to charge any fees required to Deposit Account No. 08-1394. As identified in the attached Certificate of Service, a copy of the present Rebuttal Brief, in its entirety, is being served to the address of the attorney or agent of record.

Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: September 13, 2013
HAYNES AND BOONE, LLP
IP Section, 2323 Victory Avenue,
Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Facsimile: 214/200-0853
R-342820_1.docx



V. Certificate of Service

The undersigned certifies that a copy of the THIRD PARTY REQUESTER CISCO SYSTEMS, INC.'S REBUTTAL BRIEF was served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

the attorneys of record for the assignee of USP 7,188,180 in accordance with 37 CFR § 1.903, on September 13, 2013.

/David L. McCombs /

David L. McCombs,
Registration No. 32,271

Electronic Acknowledgement Receipt

EFS ID:	16844583
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	13-SEP-2013
Filing Date:	25-OCT-2011
Time Stamp:	10:37:51
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		3PR_Rebuttal_Brief_13_Sept_2013.pdf	331374 db5bd22aa82066946875a0274a28ec2ab45391a4	yes	16

Multipart Description/PDF files in .zip description			
Document Description	Start	End	
Rebuttal Brief - Requester	1	15	
Reexam Certificate of Service	16	16	
Warnings:			
Information:			
Total Files Size (in bytes):		331374	
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>			



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.
-----------------	-------------	----------------------	---------------------	------------------

95/001,792	10/25/2011	7,188,180	43614.100	1972
------------	------------	-----------	-----------	------

22852 7590 08/16/2013
 FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
 LLP
 901 NEW YORK AVENUE, NW
 WASHINGTON, DC 20001-4413

EXAMINER

HUGHES, DEANDRA M

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 <i>Inter Partes</i> Reexamination	Control No.	Patent Under Reexamination	
	95/001,792	7,188,180	
	Examiner	Art Unit	
	DEANDRA HUGHES	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219

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.

Inter Partes Reexamination Examiner's Answer	Application No.	Applicant(s)	
	95/001,792	7,188,180	
	Examiner	Art Unit	
	DEANDRA HUGHES	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Incorporation by Reference of the Right of Appeal Notice

The Right of Appeal Notice (RAN) mailed on 12 April 2013, including all of the grounds of rejection, determinations of patentability, and explanations set forth in the RAN is incorporated by reference. Every ground of rejection and every determination not to make a proposed rejection set forth in the RAN are being maintained by the examiner.

This examiner's answer does not contain any new ground of rejection and any new determination not to make a proposed rejection.

Status of Amendment After Action Closing Prosecution

The amendment(s) filed on _____ has/have been entered.
The amendment(s) filed on _____ has/have not been entered.

Period for providing a Rebuttal Brief

Appellant(s) is/are given a period of ONE MONTH from the mailing date of this examiner's answer within which to file a rebuttal brief in response to the examiner's answer. Prosecution otherwise remains closed.

The rebuttal brief of the patent owner may be directed to the examiner's answer and/or any respondent's brief. The rebuttal brief of the third party requester(s) may be directed to the examiner's answer and/or the respondent's brief of the patent owner. The rebuttal brief must (1) clearly identify each issue, and (2) point out *where* the issue was raised in the examiner's answer and/or in the respondent's brief. In addition, the rebuttal brief must be limited to issues raised in the examiner's answer or in the respondent's brief. The time for filing the rebuttal brief may not be extended. No further submission (other than the rebuttal brief(s)) will be considered, and any such submission will be treated in accordance with 37 CFR 1.939 and MPEP 2667.

Attachment(s)

Other:
This answer is in response to Third Party Requester's Appeal Brief filed June 28, 2013 and Patent Owner's Respondent Brief filed July 29, 2013.

All correspondence relating to this *inter partes* reexamination proceeding should be directed to the **Central Reexamination Unit** at one of the following addresses:

Please mail any communications to:
Attn: Mail Stop "Inter partes Reexam"
Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Please hand-deliver any communication to:
Customer Service Window
Attn: Central Reexamination Unit
Randolph Building, Lobby Level
401 Dulany Street
Alexandria VA 22314

Please FAX any communications to: (571) 273-9900

Signed:
/Deandra M. Hughes/
Reexamination Specialist AU3992

Conferees:
/Albert Gagliardi/
Reexamination Specialist AU3992

/Sudhanshu C. Pathak/
SPRS, 3992

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
Victor Larson et al.) Control No.: 95/001,792
U. S. Patent No. 7,188,180) Group Art Unit: 3992
Issued: March 6, 2007) Examiner: Deandra M. Hughes
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK)

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed please find the following:

1. Patent Owner's Respondent Brief (14 pages);
2. Evidence Appendix (2 pages);
3. Exhibits Listed on the Evidence Appendix;
4. Related Proceedings Appendix (1 page);
5. Decisions Listed on the Related Proceedings Appendix; and
6. Certificate of Service (2 pages).

Please grant any extension of time and charge any additional fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 29, 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.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK)

Mail Stop Appeal Brief – Patents
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 Respondent Brief (14 pages);
3. Evidence Appendix (2 pages);
4. Exhibits Listed on the Evidence Appendix;
5. Related Proceedings Appendix (1 page);
6. Decisions Listed on the Related Proceedings Appendix; and
7. Certificate of Service (2 pages);

were served by first-class mail on July 29, 2013, on counsel for the third party Requester at the following address:

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: July 29, 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.: 95/001,792
)
U.S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK)
)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PATENT OWNER'S RESPONDENT BRIEF

TABLE OF CONTENTS

I. Introduction..... 1

II. Real Party in Interest..... 1

III. Related Appeals and Interferences..... 1

IV. Status of Claims 3

V. Status of Amendments 3

VI. Summary of Claimed Subject Matter 3

VII. Issues to Be Reviewed on Appeal..... 3

VIII. Argument 3

 A. Issue 1 – *Kiuchi* Does Not Anticipate Claims 1, 17, and 33..... 4

 1. *Kiuchi* Does Not Disclose “Sending an Access Request Message to the Secure Computer Network Address Using a Virtual Private Network Communication Link” 4

 2. The Examiner’s Analysis Regarding the “Sending an Access Request Message” Feature Was Consistent with the ’180 Patent..... 5

 3. The Examiner’s Construction of Virtual Private Network Is Consistent with the District Court’s Construction 6

 4. Cisco’s New Arguments Regarding HTTP/1.0 Requests Are Improper and Incorrect 6

 B. Issue 1 – *Kiuchi* Does Not Anticipate Claims 6, 22, and 37..... 7

 C. Issue 1 – *Kiuchi* Does Not Anticipate Claims 8, 24, and 39..... 8

 D. Issue 1 – *Kiuchi* Does Not Anticipate Claims 13, 15, 29, and 31..... 8

 E. Remaining Withdrawn Rejections for Issue 1 9

 F. Issues 2 and 3 – Objective Facts Demonstrate Nonobviousness 9

 1. Long-Felt Need, Failure of Others, Skepticism, Commercial Success, and Praise and Acceptance by Others Demonstrate Nonobviousness 9

 2. The Examiner Incorrectly Discounted the Evidence of Nonobviousness 12

a.	The Examiner Erred by Finding No Nexus Between the Objective Indications of Nonobviousness and the Claimed Invention	12
b.	The Examiner Erred by Applying an Unreasonable Standard for Evaluating Licenses	13
IX.	Conclusion	14

The Evidence Appendix and Related Proceedings Appendix follow the Conclusion.

I. Introduction

In response to Cisco's Appeal Brief and in view of the Right of Appeal Notice dated April 12, 2013 ("RAN") confirming all claims at issue (1, 4, 6-15, 17, 20, 22-31, 33, 35, and 37-41)¹ of U.S. Patent No. 7,188,180 ("the '180 patent"), VirnetX Inc., the owner of the '180 patent, files this Respondent Brief and submits a fee of \$2,000.00 as required under 37 C.F.R. § 41.20(b)(2)(ii).

If any additional fees are required or if the enclosed payment is insufficient, please charge the required fees to Deposit Account No. 06-0916.

II. Real Party in Interest

The real party in interest is VirnetX Inc., the assignee of record.

III. Related Appeals and Interferences

The following cases are or may be deemed related pursuant to 37 C.F.R. § 41.68(b)(1)(ii).

PTO Appeals Involving the Munger Family²

Application/Control No.
13/049,552
95/001,746
95/001,788
95/001,789
95/001,851
95/001,856

Inter Partes Review Petitions Involving the Munger Family³

Case No.
IPR2013-00348
IPR2013-00349
IPR2013-00354
IPR2013-00375
IPR2013-00376

¹ See Section IV below for a discussion of why claims 16 and 32 were never properly subject to reexamination.

² "Munger family" refers to the family of patents or patent applications related to the '180 patent.

³ As of the filing of this brief, the Office has not instituted any of these *inter partes* reviews, although filing dates have been accorded in each.

Case No.
IPR2013-00377
IPR2013-00378
IPR2013-00393
IPR2013-00394
IPR2013-00397
IPR2013-00398

Prior Judicial Proceedings Involving this Patent and/or Other Patents in the Munger Family

Title	Case No. & Forum
<i>VirnetX Inc. and Science Applications Int'l Corp. v. Microsoft Corp.</i>	No. 6:07-cv-00080 (E.D. Tex.)
<i>VirnetX Inc. v. Microsoft Corp.</i>	No. 6:10-cv-00094 (E.D. Tex.)
<i>In the Matter of Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing the Same</i>	337-TA-818 (Int'l Trade Comm'n)
<i>In the Matter of Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing the Same</i>	337-TA-858 (Int'l Trade Comm'n)

Pending Judicial Proceedings Involving this Patent and/or Other Patents in the Munger Family

Title	Case No. & Forum
<i>VirnetX Inc. and Science Applications Int'l Corp. v. Cisco Systems, Inc., Apple Inc., Aastra USA, Inc., Aastra Technologies Ltd., NEC Corp., and NEC Corp. of America</i>	No. 6:10-cv-00417 (E.D. Tex.)
<i>VirnetX Inc. and Science Applications Int'l Corp. v. Mitel Networks Corp., Mitel Networks, Inc., Siemens AG, Siemens Corp., Siemens Enterprise Communications GmbH & Co. KG, Siemens Communications, Inc., Siemens Enterprise Communications, Inc., and Avaya Inc.</i>	No. 6:11-cv-00018 (E.D. Tex.)
<i>VirnetX Inc. v. Apple Inc.</i>	No. 6:11-cv-00563 (E.D. Tex.)
<i>VirnetX Inc. and Science Applications Int'l Corp. v. Apple Inc.</i>	No. 6:12-cv-00855 (E.D. Tex.)
<i>VirnetX Inc. and Science Applications Int'l Corp. v. Apple Inc.</i>	No. 6:13-cv-00211 (E.D. Tex.)
<i>VirnetX Inc. and Science Applications Int'l Corp. v. Microsoft Corp.</i>	No. 6:13-cv-00351 (E.D. Tex.)

IV. Status of Claims

Claims 1, 4, 6-15, 17, 20, 22-31, 33, 35, and 37-41 have been confirmed. No other claims were subject to reexamination. Cisco's statement of the status of the claims is incorrect because claims 16 and 32 were not subject to reexamination. The Director found no reasonable likelihood that requester would prevail with respect to claims 2 and 18, on which claims 16 and 32 respectively depend. (Order, Sept. 6, 2013, at 10-11.) Thus, claims 16 and 32 were never properly subject to reexamination. (Second OA at 16.)

V. Status of Amendments

Cisco's statement of the status of amendments is correct. No amendments were made during reexamination.

VI. Summary of Claimed Subject Matter

Claims 1, 17, and 33 are the independent claims on appeal and the only independent claims in the '180 patent. While Cisco properly quotes the language of claim 1, VirnetX disputes Cisco's narrative summary of the claimed subject matter because it is incomplete or incorrect. For example, Cisco's description omits the step of sending a query message to a secure domain name service and the step of receiving from the secure domain name service a response message. (*See, e.g.*, '180 patent 51:45-50, Figs. 33, 34.) Cisco's description also omits the claim feature of receiving the secure network address *corresponding to the secure domain name*. (*See, e.g., id.* at 52:27-40, Figs. 33, 34.) Cisco's description also inaccurately divides the feature of sending an access request message to the secure computer network address *using a virtual private network communication link*. (*See, e.g., id.* at 52:55-62, Figs. 33, 34.)

VII. Issues to Be Reviewed on Appeal

VirnetX agrees with Cisco's statement of the issues.

VIII. Argument

The Office initially denied Cisco's Request for Reexamination in its entirety. (Decision, Dec. 17, 2011.) The Decision was consistent with the '180 patent's history of success in district court actions and before the Office in reexamination. For example, in an action against Microsoft Corporation in the Eastern District of Texas, a jury found the asserted claims of the '180 patent infringed and not invalid. (Ex. A-1.) Microsoft also sought reexamination of the '180 patent. All claims were confirmed. (*See* Control No. 95/001,270.)

After the Office denied Cisco's reexamination request, Cisco petitioned for review. The Director reaffirmed that there was no reasonable likelihood that Cisco would prevail on the majority

of the proposed rejections, and granted reexamination on only a subset of the '180 patent claims based on three issues proposed by Cisco, all of which involved *Kiuchi*. (Order, Sept. 6, 2013.) Following VirnetX's Response and Cisco's Comments after the First Office Action, the Examiner withdrew all of the rejections. (Second OA at 1.) Cisco appeals the Examiner's withdrawal of those rejections. (*See* Cisco Br. at 3.)

For at least the reasons discussed below and in VirnetX's Response, the Examiner correctly withdrew these rejections.

A. Issue 1 – *Kiuchi* Does Not Anticipate Claims 1, 17, and 33

The Examiner correctly withdrew the rejection of claims 1, 17, and 33 under 35 U.S.C. § 102 based on *Kiuchi*. (Second OA at 3-7; RAN at 3-7.)

1. *Kiuchi* Does Not Disclose “Sending an Access Request Message to the Secure Computer Network Address Using a Virtual Private Network Communication Link”

The Examiner correctly determined that *Kiuchi* does not disclose “sending an access request message to the secure computer network address using a virtual private network communication link,” as recited in claims 1, 17, and 33. Cisco contends that a request for connection, encrypted with a public key, corresponds to sending an access request message “using a virtual private network communication link.” (Cisco Br. at 8.) But as the Examiner correctly found, at the time a request for connection is sent in *Kiuchi* from a client-side proxy to a server-side proxy, the client-side proxy has no established “link” to any server-side proxy or to any C-HTTP network. (*Kiuchi* 64-65, step 3 “Request for connection”; Second OA at 3-5; Response at 5-7.) Rather, when a request for connection is sent, the proxies have simply begun the lengthy process of working towards establishing a connection to each other. (Second OA at 3-5; Response at 5-7, describing the remaining steps for creating a C-HTTP connection.) Thus, the request for connection in *Kiuchi* is not sent using any virtual private network communication link.

The Examiner also correctly rejected Cisco's argument that a one-way communication protected with a public key constitutes a “virtual private network communication link.” (Second OA at 4-5, quoting Keromytis Decl. ¶ 23; Response at 6-7.) As the Examiner recognized, public key encryption in *Kiuchi* does not create a “virtual private network communication link” in part because no “link” exists when a public-key-protected request for connection is sent. (Second OA at 4-5; Response at 6-7; Keromytis Decl. ¶¶ 21-25.) VirnetX and its expert, Dr. Keromytis, also explained that a person of ordinary skill in the art would not have understood a mere point-to-point communication between unconnected computers to constitute a virtual private network

communication link. (Response at 7; Keromytis Decl. ¶ 24.) Cisco cites no expert testimony or other evidence in rebuttal. And consistent with this understanding of a virtual private network communication link, the '180 patent recognizes and distinguishes conventional public key schemes, such as that described in *Kiuchi*. (Response at 7; Keromytis Decl. ¶ 25, citing and comparing the '180 patent 40:6-14 and *Kiuchi* 65.)

Thus, the Examiner correctly determined that *Kiuchi* does not disclose “sending an access request message to the secure computer network address using a virtual private network communication link.” (Second OA at 5.)

2. The Examiner’s Analysis Regarding the “Sending an Access Request Message” Feature Was Consistent with the '180 Patent

Cisco mistakenly contends that the Examiner’s analysis was “contrary to the '180 patent.” (Cisco Br. at 9.) This argument is based on Cisco’s misunderstanding that if a virtual private network communication link exists before an “access request message” is sent, then the virtual private network communication link *must also be established* before the prior step of “sending a query message to a secure domain name service . . . requesting . . . a secure computer network address corresponding to the secure domain name.” (Cisco Br. at 9.)

Cisco is incorrect, as the '180 patent does in fact disclose embodiments in which a virtual private network communication link is established *after* “sending a query message to a secure domain name service,” *but before* “sending an access request message to the secure computer network address.” For example, in one such embodiment, a software module on a client computer first sends a query to a secure domain name service (SDNS) in step 3408. ('180 patent 51:45-50.) In the next step (3409), the SDNS facilitates the creation of a VPN between the client computer and a secure server computer. (*Id.* at 52:27-33, “thereby creating the VPN.”) After the VPN has been created, the SDNS returns a secure network address to the software module on the client computer in step 3410. (*Id.* at 52:38-40.) The client computer then accesses secure server 3320 through the “VPN communication link” in step 3411. (*Id.* at 52:55-57.) The Examiner’s analysis of the plain claim language is accordingly consistent with the teachings of the '180 patent.

Moreover, Cisco inaccurately characterizes the portion of the '180 patent it cites in its brief. (Cisco Br. at 9, citing '180 patent 41:46-47.) There, a DNS proxy receives a DNS look-up request in step 2701. ('180 patent 41:24-25.) Following a successful determination that access to a secure computer was requested and that the user has sufficient security authorizations, a “secure VPN” is established. (*Id.* at 41:25-47.) Cisco characterizes this VPN establishment as a “final step.” (Cisco Br. at 9.) But missing from Cisco’s analysis is the fact that no “sending an access request message”

occurs before the establishment of the VPN, as Cisco implies. Thus, this portion of the '180 patent does not support Cisco's argument, as the VPN is not established after "sending an access request message." It is also not inconsistent with the language of the claims, which plainly recite sending an access request message "using a virtual private network communication link."

Cisco's arguments misread the '180 patent and the plain claim language, and are accordingly incorrect.

3. The Examiner's Construction of Virtual Private Network Is Consistent with the District Court's Construction

The Examiner properly found that a network is not a "virtual private network" unless it provides a form of privacy. (RAN at 4, "the claim term 'private' modifies the claim term 'network' and as such, *Kiuchi* much teach the 'privacy' of the 'network' and not just the privacy of the 'communication link' to anticipate the claims."). This is unremarkable since the claim term itself recites that the network is private. Nonetheless, Cisco alleges error in the Examiner's construction, arguing that the "Examiner adds a narrowing limitation to the claims by finding a requirement for an *entirely private network*." (Cisco Br. at 6, emphasis in original.) Nowhere, however, does the Examiner expressly or implicitly require anything other than what the claim says. Indeed, the Examiner's construction is based on the fact that "private" modifies "network" in the claims (RAN at 4), and Cisco has not provided any basis in logic or grammar demonstrating that "private" modifies anything other than "network."

Without a basis in the claim language, Cisco attempts to show error by arguing inconsistency between district court constructions and the Examiner's construction. (Cisco Br. at 5-6.) There is no inconsistency. In the order initiating reexamination, the Office noted that "the claim term 'private' modifies the claim term 'network.'" (Order at 8, 15, 16.) Likewise, the district court explained that a virtual private network is a "network of computers which privately communicate with each other . . ." (Cisco Br. Ex. F at 13, emphasis added.) While expressed slightly differently, both approaches require an element of privacy for the network, which refutes Cisco's allegations of inconsistency regarding privacy. Accordingly, Cisco's assertions of claim construction error are unfounded.

4. Cisco's New Arguments Regarding HTTP/1.0 Requests Are Improper and Incorrect

Cisco's HTTP/1.0 request argument is brand new, raised for the first time on appeal. Until Cisco filed its appeal brief, it had relied on *Kiuchi's* request for connection as the claimed "access request message." (See, e.g., Req. Ex. E-2 at 13-14, "The request for connection is an 'access request message' as recited in the claim," emphasis added.) Now Cisco contends for the first time that an

HTTP/1.0 request (rather than a request for connection) corresponds to the “access request message” recited in claims 1, 17, and 33. (Cisco Br. at 9-10.) But Cisco never proposed or obtained reexamination based on this feature of *Kiuchi*. (See Req. Ex. E-2 at 13-14.) Nor did Cisco ever raise this new proposed rejection in responding to VirnetX’s arguments. (See Comments at 1-2.) The Examiner also never advanced any rejection based on any HTTP/1.0 request. (See First OA at 1; Second OA at 3-7; RAN at 3-7.) Thus, Cisco’s new proposed rejection raised in its Appellant Brief is improper and outside the scope of appeal. 37 C.F.R. § 41.67(c)(1)(vi).

Under the regulation governing appellant briefs, “No new ground of rejection can be proposed by a third party requester appellant.” *Id.* The regulation provides an exception to this rule only if (1) such new ground of rejection was withdrawn by the examiner during the prosecution of the proceeding; and (2) the third-party requester has not yet had an opportunity to propose it as a third-party requester proposed ground of rejection. (*Id.*) That exception does not apply here. The Examiner never withdrew this new ground of rejection (as it never adopted such a position in the first place), and Cisco had an opportunity to propose it in the Request. Accordingly, Cisco’s new proposed rejection is outside the scope of appeal, and should be dismissed.

Moreover, Cisco’s new proposed rejection is meritless. An HTTP/1.0 request to access a webpage does not disclose any feature of claims 1, 17, and 33. Each of these claims recites “a method for accessing a secure computer network address,” wherein the final step of the method includes “sending an access request message to the secure computer network address.” Cisco’s alleged HTTP/1.0 request has nothing to do with “accessing a secure computer network address,” nor an “access request message.”

Cisco relies on the IP address of a server-side proxy as corresponding to a “secure computer network address.” (Req. Ex. E-2 at 12-13.) But *Kiuchi* does not describe any HTTP/1.0 request used in accessing the IP address of a server-side proxy—*Kiuchi* instead employs a “request for connection.” (*Kiuchi* at 65-66, steps 3 and 4, evaluating whether “access is permitted.”) By comparison, the alleged HTTP/1.0 request is simply a “request to access a web page” after a server-side proxy and a client-side proxy have already coordinated access. (Cisco Br. 10; *Kiuchi* at 66, step 6.) An HTTP/1.0 request accordingly fails to disclose “accessing a secure computer network address” or an “access request message,” because when an HTTP/1.0 request is sent in *Kiuchi*, the IP address of the server-side proxy has already been accessed via a request for connection. (*Kiuchi* at 65-66, compare steps 3 and 4 with step 6.)

B. Issue 1 – *Kiuchi* Does Not Anticipate Claims 6, 22, and 37

The Examiner properly withdrew the rejection of claims 6, 22, and 37 based on *Kiuchi*.

(RAN at 7-9.) Cisco mischaracterizes the Examiner's position in claiming that the Examiner agreed that C-HTTP version information (i.e., merely the version number) constituted a "predetermined level of service." The Examiner never agreed with Cisco's argument. (*Id.* at 8-9.) The Examiner's withdrawal of the rejection should accordingly be affirmed, as Cisco presents no arguments regarding the "version information" to the contrary.

C. Issue 1 – *Kiuchi* Does Not Anticipate Claims 8, 24, and 39

The Examiner properly determined that *Kiuchi* does not disclose a "moving window of values," and rejected Cisco's arguments as "premised on an erroneous claim construction." (RAN at 9-10.) Cisco's argument in its Appeal Brief again improperly reads the word "window" out of the claim term "moving window of valid values," contending that "the claim merely recites a 'moving window,' and thus . . . it does not matter how the nonce values vary from one to the next; it is enough that they are moving." (Cisco Br. at 12-13.) To the contrary, the claim language states that it is the "window of valid values" that is moving, not any particular nonce value. Moreover, as the Examiner and VirnetX's expert explained, *Kiuchi* nowhere discloses comparing a nonce value to any "moving window," and in fact there are many different ways that a nonce value could be checked other than comparing it to a "moving window of valid values." (RAN at 9-10, citing Keromytis Decl. ¶¶ 29-30.) Thus, the features of claims 8, 24, and 39 are neither disclosed by, nor inherent in, *Kiuchi*.

D. Issue 1 – *Kiuchi* Does Not Anticipate Claims 13, 15, 29, and 31

The Examiner correctly withdrew the rejections of claims 13, 15, 29, and 31 based on the patentability of confirmed independent claims 1 and 17, but incorrectly found that *Kiuchi* discloses the various features of claims 1 and 17 occurring "at the client computer" or "performed by a client computer." (RAN at 15-16.) In particular, the Examiner incorrectly interpreted VirnetX's arguments as relying on a "firewall" feature to distinguish *Kiuchi*, rather than relying on the separateness of *Kiuchi*'s client computers and its proxies (e.g., the client- and server-side proxies). (*See id.* at 16.)

A person of ordinary skill would not have understood *Kiuchi* to disclose a client computer that performs the features of *Kiuchi* alleged to correspond to the steps of claims 1 and 17. (Response at 12-13; Keromytis Decl. ¶¶ 36-38.) For example, Cisco and the Examiner only contended that the *client-side proxy* receiving the IP address of the server-side proxy corresponds to the claim feature of "receiving from the secure domain name service a response message containing the secure network address corresponding to the secure domain name." (Req. Ex. E-2 at 12-13; First OA at 1.) Thus, no client computer in *Kiuchi* performs the steps allegedly corresponding to claims 1 and 17. Claims 13, 15, 29, and 31 are accordingly patentable for this additional reason.

A client computer and a client-side proxy also cannot properly be conflated, because the

firewall setup of *Kiuchi* illustrates that a client-side proxy and a client computer *are not the same computer*. (Keromytis Decl. ¶¶ 37-38, citing *Kiuchi* 64; Response at 12-13.) *Kiuchi*'s C-HTTP system is specifically designed for proxy-to-proxy security (rather than end-to-end security), (*Kiuchi* at 67-68), and user agents/client computers and origin servers are accordingly absent from much of the C-HTTP setup process between the proxies, (*id.* at 65-67).

E. Remaining Withdrawn Rejections for Issue 1

The Examiner correctly withdrew the remaining rejections presented in issue 1, at least because the claims involved in those proposed rejections (4, 9, 10, 12, 14, 20, 24, 26, 28, 30, 35, and 40) depend from one or more allowable claims. (*See, e.g.*, RAN at 25.)

F. Issues 2 and 3 – Objective Facts Demonstrate Nonobviousness

The Examiner correctly withdrew the obviousness rejections of claims 7, 11, 23, 27, 38, and 41, at least because they depend from one or more allowable claims. (*See id.*) These claims are also patentable because several objective facts demonstrate nonobviousness.

These objective facts are sometimes called “secondary considerations,” but they are not merely afterthoughts or rebuttal evidence. Instead, they “guard as a check against hindsight bias” and they must be considered before ever reaching a conclusion of obviousness. *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1079 (Fed. Cir. 2012). Secondary considerations supporting nonobviousness include long-felt need, failure of others, skepticism, commercial success, and praise and acceptance by others in the field. *Graham v. John Deere Co.*, 383 U.S. 1 (1966); M.P.E.P. § 2145. Each of these considerations applies to the claims in Issues 2 and 3.

1. Long-Felt Need, Failure of Others, Skepticism, Commercial Success, and Praise and Acceptance by Others Demonstrate Nonobviousness

Long-Felt Need

Demonstrating a long-felt need, the computer-security and internet-security industries have long sought ways to conveniently establish secure communication links, such as VPN communication links. At the time of the effective filing date of the '180 patent, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. (Short Decl. ¶¶ 8, 11; Ex. B-4 at 1.) It 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. (Short Decl. ¶ 11; Ex. B-4 at 1.) 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. (Short Decl. ¶ 9; Ex. B-4 at 1-2.) The inventions claimed in the '180 patent combine both the ease of use *and* the security aspects of a VPN, without sacrificing one or the other. One way they do this is through a method for accessing a secure computer network address that involves establishing a VPN communication link, and then sending an access request message to a secure computer network address using the VPN communication link. (Short Decl. ¶¶ 3, 9; Ex. B-4 at 1-2; Ex. B-1 at 1-2.)

Before the inventions claimed in the '180 patent, there was a long-felt need for a system that could establish a VPN communication link in a simple and straightforward manner, as “a solution that was difficult for an end-user to employ would likely lead to a lack of use or incorrect use.” (Short Decl. ¶ 3.) 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. (*Id.* at ¶¶ 4-5; *see* Ex. B-1 at VNET00219302, 319-321; Ex. B-2 at VNET00219244, 284, 298-299, 593, 625.) One such program, “Next Generation Internet,” received approximately \$130 million in funding between 1998 and 2000. (Short Decl. ¶ 4; Ex. B-1 at VNET00219302, 319-321.)

Recognizing this long-felt need for these inventions, both In-Q-Tel, a venture capital firm that invests in companies developing cutting edge technology, and SAIC (the original owner of the '180 patent) also spent significant resources on their development. (Short Decl. at ¶¶ 6-7.) In fact, in the year the inventions claimed in the '180 patent were developed, SAIC spent approximately 85% of its research and development budget for that year on developing these and other similar inventions. (*Id.* at ¶ 7.)

Failure of Others

Given the long-felt need in the industry, it is not surprising others attempted to create an easy-to-use VPN solution. Those attempts failed. For example, the DARPA-funded research programs discussed above fell far short of the claimed inventions of the '180 patent. (*Id.* at ¶¶ 4-5, 10.) One such program, “Dynamic Coalitions,” was specifically created to address the ability of the Department of Defense to quickly and easily set up secure communications over the Internet. (*Id.* at ¶ 5.) More than 15 prestigious organizations took part in the “Dynamic Coalitions” research program, but none of them came up with a solution in the relevant time frame that was even close to providing the ease of use of the solutions provided in the claimed

inventions of the '180 patent. (*Id.*; Ex. B-3 at 1-4.) They did not develop a solution that allowed a user to easily and conveniently enable secure communications. (Short Decl. ¶ 5; Ex. B-3 at 1-4.) By employing a method for accessing a secure computer network address that involves establishing a VPN communication link, and then sending an access request message to a secure computer network address using the VPN communication link, the inventions of the '180 patent succeeded where others failed. (Short Decl. ¶ 11; Ex. B-1 at 1-2.)

Skepticism

Given the failure of others to achieve the feats made possible by the inventions of the '180 patent, the technology of the '180 patent was also met with skepticism by those skilled in the art who learned of the patented inventions. (Short Decl. ¶ 15.) For example, a DARPA program manager informed one of the co-inventors of the '180 patent that technology disclosed in the '180 patent would never be adopted. (*Id.*) Moreover, the IT offices of many large companies and institutions expressed skepticism that secure connections could ever be enabled easily by regular computer users. (*Id.*) The skepticism is understandable, as the claimed inventions of the '180 patent were contrary to the accepted wisdom at the time of the inventions. (*Id.* at ¶ 13.) There was a pervasive understanding in the industry that reliable security could only be achieved through difficult-to-provision VPNs and that easy-to-set-up connections could not be secure. (*Id.*; *see also* Ex. B-5.)

Commercial Success

Due to the breakthrough the inventions of the '180 patent achieved, the claimed inventions have experienced commercial success, with multiple companies licensing the technology. For example, 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 '180 patent in July 2002. (Short Decl. ¶ 12.) SafeNet licensed the patents because of features disclosed and claimed in the patents, including those ultimately claimed in the '180 patent. (*Id.*) Similarly, Microsoft Corporation; Aastra USA, Inc.; Mitel Networks Corporation; NEC Corporation; and NEC Corporation of America have entered into portfolio licenses that include the '180 patent. (*Id.*)

Praise and Acceptance by Others

Those in the industry have also praised the inventions, either by stating their praise or by

demonstrating praise through their conduct, such as by investing in the technology or licensing it. For example, SAIC invested a disproportionately large percentage of its internal resources in the technology. (Short Decl. ¶ 7.) SafeNet and Microsoft have both licensed the technology. (*Id.* at ¶¶ 12, 16) A study done by CSMG praised the inventions. (*Id.* at ¶ 16.) And Jim Rutt at Network Solutions, which was eventually acquired by Verisign, praised and expressed significant interest in the technology and would have invested but for a change in circumstances at his company. (*Id.*) Each of these facts objectively demonstrates that the claimed inventions were not merely obvious variations of earlier technology. Instead, they represent a breakthrough that has been widely adopted.

2. The Examiner Incorrectly Discounted the Evidence of Nonobviousness

Despite being presented with a wealth of evidence, the Examiner dispensed with these facts by contending that the “[evidence] lacks the requisite nexus with the claimed language.” (RAN at 20-24.) He also set forth an incorrect legal test for whether licensing supports nonobviousness. Accordingly, the Examiner primarily erred in two ways: (1) finding no nexus between the facts and the claimed invention; and (2) creating unreasonable standards for determining whether licensing supports nonobviousness.

a. The Examiner Erred by Finding No Nexus Between the Objective Indications of Nonobviousness and the Claimed Invention

While the claims as a whole define the invention, the claimed inventions generally pertain to methods and computer-readable media for accessing a secure computer network address by “sending an access request message to the secure computer network address using a virtual private network communication link.” As the ’180 patent explains, this technique allows a user to initiate the creation of a VPN communication link, which is established before accessing a secure computer network address. (’180 patent 52:27-33.) In allowing a user to easily establish a VPN communication link before accessing a secure computer network address, this technique utilizes top-level domain names as claimed in claims 11, 27, and 41. (*Id.* at 51:46-50.) The ’180 patent further specifies that “[p]referably, such a VPN communication link can be based on . . . an IP address hopping regime that pseudorandomly changes IP addresses in packets,” as claimed in claims 7, 23, and 38. (*Id.* at 51:52-57.) Accordingly, the invention claimed in the ’180 patent allows a user to easily establish a VPN communication link—a feature

not found in the prior art. VirnetX's evidence of secondary considerations is directly linked to this benefit, which flows from the claimed features and therefore has a nexus with the claimed invention. (*See generally* Short Decl., repeatedly addressing this benefit.)

The Examiner found that VirnetX's "evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation." (RAN at 22, 23.) The Examiner is incorrect. Each of the claims recites features that allow a user to easily establish a VPN communication link. VirnetX's claims are directed to features that allow this to happen, including the sending of "an access request message to the secure computer network address using a virtual private network communication link." This feature is found in every claim of the '180 patent, and is not limited to a single claim. In addition, VirnetX's arguments are not limited to that feature. Other aspects of the claims also support this easy VPN creation, including the use of top-level domain names and a computer network address hopping regime.

The Examiner provided only a short explanation of why he found a nexus lacking, but it appears that the Examiner may have found no nexus because the evidence does not use the identical language recited in the claims. The Examiner relied on no authority requiring identical language, however, and in fact such identity is not required. Rather, the Federal Circuit has repeatedly found a nexus where the evidence of secondary considerations pertains to benefits flowing from the claimed invention, even if those benefits are not expressly recited in the claims. *See, e.g., In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d at 1083 (long-felt need for a pharmaceutical product that did not require multiple daily doses, which was a feature that flowed from the claimed invention, supported nonobviousness); *Transocean Offshore Deepwater Drilling*, 699 F.3d at 1354 (long-felt need for greater drilling efficiency, which flowed from the claimed invention, supported nonobviousness). Consequently, the Examiner was incorrect in not finding a nexus between the evidence and the claimed invention.

b. The Examiner Erred by Applying an Unreasonable Standard for Evaluating Licenses

The Examiner held VirnetX's licensing proof to an unreasonable standard not required by law. The Examiner relied on speculation that other "market factors" may have led to VirnetX's licensing of the '180 patent to Microsoft, SafeNet, Aastra, Mitel, NEC Corporation, and NEC Corporation of America. (RAN at 22.) For example, the Examiner contended that perhaps "superior business acumen or marketing" or "a desire to avoid the costs of litigation" precipitated

Evidence Appendix

Pursuant to 37 C.F.R. § 41.68(b)(1)(viii), VirnetX submits the following evidence in support of its appeal:

Exhibit No.	Description	Comments
DEC-1	Declaration of Angelos D. Keromytis, Ph.D. dated December 16, 2012 ("Keromytis Decl.")	Submitted on December 19, 2012 with the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.
DEC-2	Declaration of Dr. Robert Dunham Short III ("Short Decl.")	Submitted on December 19, 2012 with the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.
A-1	Verdict Form from VirnetX Inc. v. Microsoft Corp., No. 6:07-cv-00080 (E.D. Tex.)	Submitted on December 19, 2012 with the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.
B-1	Excerpt from Department of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999	Submitted on December 19, 2012, as Exhibit B-1 to the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.
B-2	Collection of Reports and Presentations on DARPA Projects	Submitted on December 19, 2012, as Exhibit B-2 to the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.
B-3	Maryann Lawlor, <i>Transient Partnerships Stretch Security Policy Management</i> , SIGNAL Magazine (Sept. 2001), http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes	Submitted on December 19, 2012, as Exhibit B-3 to the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.

Exhibit No.	Description	Comments
B-4	Joel Snyder, <i>Living in Your Own Private Idaho</i> , Network World (January 26, 1998), http://www.networkworld.com/intranet/0126review.html	Submitted on December 19, 2012, as Exhibit B-4 to the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.
B-5	Tim Greene, <i>CEOs Chew the VPN Fat</i> , CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch	Submitted on December 19, 2012, as Exhibit B-5 to the Patent Owner's Response to Office Action of September 19, 2012. The Response was entered and responded to by the Examiner in the Office Action of February 27, 2013.

Related Proceedings Appendix

Pursuant to 37 C.F.R. § 41.68(b)(1)(ix), VirnetX identifies the following decisions:

Tab No.	Decisions from VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation, No. 6:07-cv-00080 (E.D. Tex.)
1	Memorandum Opinion, dated July 30, 2009
1	Order, dated February 24, 2010
1	Verdict Form, dated March 16, 2010
1	Order of Dismissal, dated June 1, 2010
Tab No.	Decisions from VirnetX Inc. v. Microsoft Corporation, No. 6:10-cv-00094 (E.D. Tex.)
2	Order of Dismissal, dated May 24, 2010
Tab No.	Decisions from VirnetX Inc. and Science Applications Int'l Corp. v. Cisco Systems, Inc., Apple Inc., Aastra USA, Inc., Aastra Technologies Ltd., NEC Corporation, and NEC Corporation of America, No. 6:10-cv-00417 (E.D. Tex.)
3	Memorandum Opinion and Order, dated April 25, 2012
3	Order of Dismissal, dated May 14, 2012
3	Order of Dismissal, dated September 20, 2012
3	Order, dated October 4, 2012
3	Order, dated October 22, 2012
3	Order, dated October 29, 2012
3	Order, dated October 29, 2012
3	Verdict Form, dated November 6, 2012
3	Memorandum Opinion and Order, dated February 26, 2013
3	Final Judgment Pursuant to Fed. R. Civ. P. 54(b), dated February 28, 2013
3	Verdict Form, dated March 14, 2013
3	Final Judgment, dated March 19, 2013
Tab No.	Decisions from VirnetX Inc. and Science Applications Int'l Corp. v. Mitel Networks Corp., Mitel Networks, Inc., Siemens AG, Siemens Corporation, Siemens Enterprise Communications GmbH & Co. KG, Siemens Communications, Inc., Siemens Enterprise Communications, Inc., and Avaya, Inc., No. 6:11-cv-00018 (E.D. Tex.)
4	Memorandum Opinion and Order, dated August 1, 2012
Tab No.	Decisions from In the Matter of Certain Devices with Secure Communication Capabilities, Components Thereof, and Products Containing the Same, 337-TA-818 (Int'l Trade Comm'n)
5	Order No. 15: Initial Determination Terminating the Investigation Due to Lack of Standing (Public Version), dated April 9, 2013
5	Notice of Commission Decision Not to Review an Initial Determination Terminating the Investigation Due to Lack of Standing and Order No. 14 Denying Complainant's Renewed Motion to Amend the Complaint and Notice of Investigation; Termination of the Investigation, dated August 20, 2012

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	Joseph Edwin Palys./Donna Beckford-Haris				
Attorney Docket Number:	43614.100				
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:					
Filing Appeal Brief Inter Partes Reexam	1404	1	2000	2000	
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				2000

Electronic Acknowledgement Receipt

EFS ID:	16441837
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Donna Beckford-Haris
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	29-JUL-2013
Filing Date:	25-OCT-2011
Time Stamp:	20:45:04
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2000
RAM confirmation Number	7784
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1		180Transmittal_COS.pdf	88311 1cab68cb737ce63021773c49a663b0ed6d087ca4	yes	3
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Trans Letter filing of a response in a reexam	1	1	
		Reexam Certificate of Service	2	3	
Warnings:					
Information:					
2	Reexam Miscellaneous Incoming Letter	180Respondent_Brief.pdf	1055808 e784d8b7ef381b8d1163d5ac87c9f52e2ae2a789	no	17
Warnings:					
Information:					
3	Reexam Miscellaneous Incoming Letter	EvidenceAppendix.pdf	114257 3d3f358ce46f31ff93fe1e8854589d1a77e9ac3	no	2
Warnings:					
Information:					
4	Reexam Miscellaneous Incoming Letter	ExhibitDEC1KeromytisDec.pdf	3181992 ef339ce1d7b5873b2709cbcbce06d16a4c12c48	no	46
Warnings:					
Information:					
5	Reexam Miscellaneous Incoming Letter	ExhibitDE2ShortDeclaration.pdf	370973 9e2611bdf34866c710a84ddf1ec807f9cc726afe	no	6
Warnings:					
Information:					
6	Reexam Miscellaneous Incoming Letter	ExhibitA1.pdf	92925 89f4b986a072bd890be2f63fce6a0f52d57c261	no	3
Warnings:					
Information:					
7	Reexam Miscellaneous Incoming Letter	ExhibitB1.pdf	1233828 f749b1bb335205db0bac42220808affd7d3ef887	no	23
Warnings:					
Information:					
8	Reexam Miscellaneous Incoming Letter	ExhibitB2.pdf	6099290 65e0dc320771a7616622487f110d18fd68882cbe	no	95

Warnings:					
Information:					
9	Reexam Miscellaneous Incoming Letter	ExhibitB3.pdf	252416 04cbaa411df05711ccd0387cce6c346cc8ddcbc1	no	5
Warnings:					
Information:					
10	Reexam Miscellaneous Incoming Letter	ExhibitB4.pdf	296256 c04b3c7f1def0bdb4c30479670a493be3b096aa3	no	5
Warnings:					
Information:					
11	Reexam Miscellaneous Incoming Letter	ExhibitB5.pdf	281789 6777caf36eead4c2dc0d93ce3e706499b75e503a	no	6
Warnings:					
Information:					
12	Reexam Miscellaneous Incoming Letter	ERelatedProceedingsAppendix.pdf	105830 a82e4de62706130e6407c8216b9164fba6abb8e16	no	1
Warnings:					
Information:					
13	Reexam Miscellaneous Incoming Letter	1_2010_03_16MicrosoftJuryVerdict.pdf	1071322 33739be92b7c6b548a388572c060b9ede69cda63	no	2
Warnings:					
Information:					
14	Reexam Miscellaneous Incoming Letter	1_2010_06_01MicrosoftDismissalOrder.pdf	942941 49760f72e80f17fa91bd1d63b14eeb20a68af075	no	2
Warnings:					
Information:					
15	Reexam Miscellaneous Incoming Letter	2_2010_05_24MicrosoftDismissalOrder.pdf	396188 f45d481fbed1dae02e8eccc044a5235130dac01a	no	1
Warnings:					
Information:					
16	Reexam Miscellaneous Incoming Letter	3_2012_05_14CiscoOrderDismissingAstra.pdf	869293 ca0e19c5ad59b63673cc7617e575010955f30844	no	2
Warnings:					
Information:					
17	Reexam Miscellaneous Incoming Letter	3_2012_09_20CiscoOrderDismissingNEC.pdf	908078 4d19b16aaa194b2f5d248cfd8962e1b08b8fa9b	no	2

Warnings:					
Information:					
18	Reexam Miscellaneous Incoming Letter	3_2012_10_04CiscoOrderGrant ingDef.pdf	517228 065020f1ac6c5d21fb99e797ee3c4e4384f c84	no	1
Warnings:					
Information:					
19	Reexam Miscellaneous Incoming Letter	3_2012_10_22CiscoOrderGrant ingPartialSummaryJudgment. pdf	12171888 ca3d2e5e4f2a493dac937e9894d35d8ade9 cec85	no	11
Warnings:					
Information:					
20	Reexam Miscellaneous Incoming Letter	3_2012_10_29CiscoOrderDenyi ngAppleMotiontoDismissInvali dity.pdf	313460 e11646e1d293640d3dd451721925063f4dc 4c4f3	no	1
Warnings:					
Information:					
21	Reexam Miscellaneous Incoming Letter	3_2012_11_06VerdictForm.pdf	790426 8205617f2c16e98186e6ff83130de984889c 0d80	no	2
Warnings:					
Information:					
22	Reexam Miscellaneous Incoming Letter	3_2013_02_28CiscoFinalJudgm entAgainstApple.pdf	1505836 4622c2fdb6e214cd328986f12d5cb95384fa 9087	no	2
Warnings:					
Information:					
23	Reexam Miscellaneous Incoming Letter	3_2013_03_19CiscoFinalJudgm entAgainstCisco.pdf	913822 de1ad8b303ca470ebfb751c0d93c260b423 3fdff	no	2
Warnings:					
Information:					
24	Reexam Miscellaneous Incoming Letter	3_2013_CiscoOrderSettingHear ingAppleMotionDismissInvalidi tyCounterclaims.pdf	750138 8d7a768ba0591f86c60da536456e1ee1ff99 6850	no	1
Warnings:					
Information:					
25	Reexam Miscellaneous Incoming Letter	4_2012_08_01MitelMarkmanOr der.pdf	12590971 3f572a80983750397ec122c44bbe2e018ecc b5d8	no	13
Warnings:					
Information:					
26	Reexam Miscellaneous Incoming Letter	5_2012_08_20NoticeofNonRevi ewofIDTerminatingInvestigatio n.pdf	2956063 ba23f3626409cf4b23520b800472f4782fd c27	no	3

Warnings:					
Information:					
27	Reexam Miscellaneous Incoming Letter	5_2013_04_09Order15IDTerminatingInvestigation.pdf	6236022 6cf6a357ed2ebfea3df829b4679bf40beb161124	no	6
Warnings:					
Information:					
28	Reexam Miscellaneous Incoming Letter	1_2009_07_30MicrosoftMarkmanOrder.pdf	5601810 8e53c76c4932aedf65a6c3a7a9837deff033a7e	no	35
Warnings:					
Information:					
29	Reexam Miscellaneous Incoming Letter	1_2010_02_24MicrosoftOrderDenyingSummaryJudgmentofNonobviousness.pdf	5620813 2b4f2149c79e738c0832c8275ae6f07ced54b273	no	35
Warnings:					
Information:					
30	Reexam Miscellaneous Incoming Letter	3_2012_04_25CiscoMarkmanOrder.pdf	5052874 1dfa2d1f141bc07afde6c682bd04d7ea5772bc55	no	31
Warnings:					
Information:					
31	Reexam Miscellaneous Incoming Letter	3_2013_02_26CiscoOrderLeadingUptoFinalJudgment.pdf	7756431 34a6e0c81e01cad949092f6d749aed621e2b06d2	no	47
Warnings:					
Information:					
32	Fee Worksheet (SB06)	fee-info.pdf	30616 0fc340fba9af731ef5bf00e3d504810ee0cf74d	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			80169895		

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

Application of: Victor Larson, et al.	§	Docket No.	43614.100
<i>Inter Partes</i> Reexamination	§	Examiner:	HUGHES, Deandra
Patent No. 7,188,180	§	Art Unit:	3992
Proceeding No.: 95/001,792	§	Conf. No.	1972

Mail Stop: *Inter Partes* Reexamination
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

THIRD PARTY REQUESTER CISCO SYSTEMS, INC.'S

APPEAL BRIEF

Table of Contents

I.	Real Party in Interest	1
II.	Related Appeals and Interferences	1
III.	Status of Claims	2
IV.	Status of Amendments	2
V.	Summary of Claimed Subject Matter	2
VI.	Issues to be Reviewed on Appeal.....	3
VII.	Argument.....	3
A.	Overview of Kiuchi	3
B.	Issue 1: Kiuchi Anticipates Claims 1, 17, and 33.....	5
1.	Claim Construction for “virtual private network”	5
2.	Kiuchi teaches “sending an access request message to the secure computer network address using a virtual private network communication link” under the broadest reasonable interpretation.....	6
C.	Issue 1: Kiuchi Anticipates Claims 6, 22, and 37.....	10
D.	Issue 1: Kiuchi Anticipates Claims 8, 24, and 39.....	12
E.	Issues 1, 2, & 3: Dependent Claims Will Fall Together with the Independent Claims	13
VIII.	Conclusion.....	14
IX.	Claims Appendix.....	15
X.	Evidence Appendix	20
XI.	Related Proceedings Appendix	22
XII.	Certificate of Service.....	23

I. Real Party in Interest

The real party in interest is Cisco Systems, Inc.

II. Related Appeals and Interferences

There are no prior or pending appeals or interferences involving the '180 Patent.

The '180 Patent is or has been the subject of the following pending litigations:

Styling	Number	District	Filed
<i>VirnetX Inc. v. Apple Inc.</i>	6-13-cv-00211	TXED	February 26, 2013
<i>VirnetX Inc. v. Cisco Systems, Inc.</i>	6-10-cv-00417	TXED	August 11, 2010
<i>VirnetX Inc. v. Microsoft Corp.</i>	6-13-cv-00351	TXED	April 22, 2013

In addition, the '180 Patent is related to—and shares some common claim terminology with—the patents in these pending *inter partes* reexaminations:

Control No.	Patent No.	Status as of June 28, 2013
95/001679 and 95/001682 (merged)	6,502,135	Office Action (Mar. 12, 2013)
95/001714 and 95/001697 (merged)	7,490,151	Awaiting next Office Action
95/001851	7,418,504	Right of Appeal Notice (Jun. 25, 2013)
95/001788	7,418,504	Right of Appeal Notice (Jun. 25, 2013)
95/001856	7,921,211	Right of Appeal Notice (Jun. 25, 2013)
95/001789	7,921,211	Right of Appeal Notice (Jun. 26, 2013)
95/001746	6,839,759	On Appeal
95/001949	8,051,181	Awaiting next Office Action

Finally, the '180 Patent is related to—and shares some common claim terminology with—the patents in these pending *inter partes* reviews:

Case No.	Patent No.	Date Filed
IPR2013-00348	6,502,135	June 12, 2013
IPR2013-00349	6,502,135	June 12, 2013
IPR2013-00354	7,490,151	June 17, 2013
IPR2013-00375	6,502,135	June 23, 2013
IPR2013-00376	7,490,151	June 23, 2013
IPR2013-00377	7,418,504	June 23, 2013
IPR2013-00378	7,921,211	June 23, 2013

III. Status of Claims

Claims 1, 4, 6-17, 20, 22-33, 35 and 37-41 are subject to reexamination and presently stand confirmed. No other claims are subject to reexamination.

IV. Status of Amendments

No claim has been amended, and there are no pending proposed amendments.

V. Summary of Claimed Subject Matter

The '180 patent has 41 total claims and three independent claims—claims 1, 17, and 33. Claim 1 describes a method for accessing a secure computer network address, while claims 17 and 33 are directed to a storage medium (claim 17) or an apparatus (claim 33) with instructions for performing substantially the same method. Thus, the body of each claim recites method steps.

At a high level, the steps of the independent claims include receiving a secure domain name, sending a query message requesting a secure computer network address associated with the secure domain name, receiving the secure computer network address, and sending an access request message to the secure computer network address. The access request message is sent using a virtual private network communication link.

Claim 1 is representative:

1. A method for accessing a secure computer network address, comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

VI. Issues to be Reviewed on Appeal

Requester-Appellant Cisco appeals all of the proposed rejections for which reexamination was ordered but now stand withdrawn or not adopted by the Examiner. Although Cisco proposed various grounds of rejection, only the following proposed rejections, based on *Kiuchi* as a primary reference, are being considered in this reexamination:

Rejections based on Kiuchi

Issue 1: Claims 1, 4, 6, 8-10, 12-15, 17, 20, 22, 24-26, 28-31, 33, 35, 37 and 39-40 are anticipated by *Kiuchi* under 35 U.S.C. § 102.

Issue 2: Claims 11, 27, and 41 are obvious over *Kiuchi* under 35 U.S.C. § 103.

Issue 3: Claims 7, 23, and 38 are obvious over *Kiuchi* in view of *Martin* under 35 U.S.C. § 103.

VII. Argument

The Examiner initially (and correctly) rejected all of the claims subject to reexamination, but then withdrew those rejections. As analyzed in greater detail below, *Kiuchi* and the other prior art references teach the limitations of the claims. The Examiner's decision to withdraw the rejections was based on the Examiner's addition of an erroneous and improper narrowing limitation. The Board should reverse the Examiner and reinstate the rejection of all claims subject to reexamination.

A. Overview of *Kiuchi*

In 1996, researchers in Japan developed and deployed a new system to facilitate secure communications among hospitals and related institutions. The system allowed members of a

closed network to easily and securely share patient information and clinical trial documents over the Internet. This work was described in detail in “C-HTTP — The Development of a Secure, Closed HTTP-based Network on the Internet,” by Takahiro Kiuchi and Shigekoto Kaihara (hereinafter, “Kiuchi”).

Quite similar to the ’180 patent, Kiuchi describes technology for establishing secure network links between computers. To accomplish this goal, Kiuchi describes a system with “a client-side proxy, a server-side proxy and a C-HTTP name server.” (Kiuchi, Abstract.) The proxies reside on a firewall at each hospital or other institution, and they “communicate with each other using a secure, encrypted protocol.” (*Id.*) Thus, the communications between the proxies use an encrypted channel. Kiuchi’s system also includes a secure name server, called the C-HTTP name server, which assists the proxies in locating each other’s network addresses.

Kiuchi teaches that a client-side proxy initiates a secure connection by first sending a request to the C-HTTP name server for the IP address of a specified server-side proxy. Kiuchi teaches that the server names resolved by the C-HTTP name server are *not* conventional domain names:

In a C-HTTP-based network, *instead of a DNS*, a C-HTTP-based secure, encrypted name and certification service is used.

(Kiuchi at 64 (emphasis added).) For example, Kiuchi provides example names for the client-side proxy and server-side proxy that are not conventional domain names:

```
1) Client-side proxy
   hostname: University.of.Tokyo.Branch.Hospital
   IP address: 130.69.111.111
2) server-side proxy
   hostname: Coordinating.Center.CSCRG
   IP address: 130.69.222.222
   port number: 8080
```

(Kiuchi at 73.) Kiuchi’s example domain names end in “.Hospital” and “.CSCRG”, whereas the ’180 patent states that standard domain names must end in “.com, .net, .org, .edu, .mil or .gov.” (’180 Patent, col. 50, l. 18.) Thus, the domain names taught by Kiuchi are *not* conventional domain names that could be resolved by a conventional domain name service. Rather, they can be resolved only by the C-HTTP name server.

After the C-HTTP name server responds with the IP address, the client-side proxy sends an encrypted connection request message to the server-side proxy:

A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL.... If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values.... When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client-side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy's public key....

(Kiuchi at 65 (emphasis added).) The client-side proxy also sends further communication requests to the server-side proxy, using encryption to protect their privacy:

6) Sending C-HTTP requests to the server-side proxy (Fig. 2g)

Once the connection is established, a client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format.

(Kiuchi at 66.)

Kiuchi further teaches that the secure, encrypted communications between the client-side proxy and the server-side proxy form a “virtual private network communication link” as recited in the ’180 patent claims. For example, Kiuchi describes the secure connections among computers as forming a “closed HTTP-based *virtual network*” that serves as a more flexible alternative to privately leased circuits. (Kiuchi at 69.)

B. Issue 1: Kiuchi Anticipates Claims 1, 17, and 33

Claim 1 recites in part, “sending an access request message to the secure computer network address using a virtual private network communication link.” Claims 17 and 33 recite similar limitations. The Examiner focused on this limitation in withdrawing the rejection of these claims as anticipated by Kiuchi. In particular, the Examiner stated that Kiuchi failed to teach “privacy” of the “network.” (RAN at 4.) The Examiner also stated that a message from a client-side proxy to a server-side proxy is a request to *establish* a virtual private network communication link, and therefore cannot be transmitted *using* such a link. (RAN at 5.) Here, the Examiner’s analysis and conclusion are incorrect.

1. Claim Construction for “virtual private network”

In litigation involving the ’180 Patent, the Patent Owner has asserted that a “virtual private network” is a “network of computers which privately communicate with each other by encrypting traffic on insecure communications paths between the computers.” (Ex. F at 13.) In

a first federal district court case, the court agreed and adopted this claim construction. (Ex. B-4 at 10.) The court also found that the words “communication” and “link” were readily understood, and therefore the phrase “virtual private network communication link” did not require construction beyond that already provided for “virtual private network.” (*Id.* at 25-26.) In a second case in the same court, virtual private network was construed as meaning a “network of computers which privately communicate with each other by encrypting traffic on insecure communications paths between the computers where the communication is both secure and anonymous.” (Ex. L at 8.)

In this proceeding, the Examiner improperly added a narrowing limitation to “virtual private network” and “virtual private network communication link” that did not exist in either of the district court cases. The Examiner did not address or acknowledge the courts’ claim constructions, providing instead the following statement:

Upon examination of **Kiuchi**, it is found the claim term 'private' modifies the claim term 'network' and as such, **Kiuchi** must teach the 'privacy' of the 'network' and not just the privacy of the 'communication link' to anticipate the claims.

(RAN at 4.) In this analysis, the Examiner adds a narrowing limitation to the claims by finding a requirement for an *entirely private network*. In contrast, the courts constructions expressly allow the claimed network to have “insecure communication paths” so long as the computers are still able to “privately communicate with each other by encrypting traffic.” Neither the district court nor VirnetX’s own proposed construction interpreted the claim as requiring “‘privacy’ of the ‘network’” as the Examiner did. Since the Examiner added this narrowing limitation not found in any court’s claim interpretation, it is irrefutable that the Examiner improperly limited the meaning of virtual private network.

2. Kiuchi teaches “sending an access request message to the secure computer network address using a virtual private network communication link” under the broadest reasonable interpretation

The Examiner’s erroneous claim interpretation led to the incorrect decision to withdraw the rejection of claim 1 as anticipated by Kiuchi. As more fully analyzed below, Kiuchi teaches sending an access request message using a “virtual private network communication link” under the broadest reasonable interpretation, which must be at least as broad as the claim interpretations advocated by the Patent Owner and adopted by the federal courts.

The Examiner demanded that to anticipate claim 1, “Kiuchi must teach the ‘privacy’ of the ‘network’ and not just the privacy of the ‘communication link.’” (RAN at 4.) In contrast, under one federal court’s interpretation, as long as communications across a link are encrypted when they transit an insecure communication path, the link is a “virtual private network communications link.” (See Ex. B-4 at 10.)

a) Kiuchi teaches “a virtual private network”

Under the broadest reasonable interpretation of the claim, Kiuchi teaches a “virtual private network.” Specifically, Kiuchi teaches “secure HTTP communication mechanisms within a closed group of institutions on the Internet.” (Kiuchi, Abstract at 64.) Each institution is “protected by its own firewall,” and Kiuchi teaches encrypting communications between “a client-side proxy on the firewall of one institution” and “a server-side proxy on the firewall of another institution.” (Kiuchi at 64.) The proxies “communicate with each other using a secure, encrypted protocol (C-HTTP).” (*Id.*) Thus, Kiuchi discloses a network of institutions in which computers privately communicate by encrypting traffic over insecure paths, such as the Internet. This network of privately communicating institutions is, under the broadest reasonable interpretation, a “virtual private network.”

b) Kiuchi teaches “a virtual private network communication link”

Under the broadest reasonable interpretation of the claim, Kiuchi teaches a “virtual private network communication link.” Specifically, Kiuchi describes a variety of communication links between computers within Kiuchi’s closed group of institutions (e.g., the “virtual private network”). These communication links, occurring within the virtual private network and over the Internet, are encrypted to ensure the privacy and security of transferred information, such as patient information. (Kiuchi at 64.) One such communication link is used to send a request for connection sent from a client-side proxy to a server-side proxy:

3) Request for connection to the server-side proxy
(Appendix 3. c)

When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client-side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy’s public key and contains the client-side proxy’s IP address, hostname, request Nonce value and symmetric data exchange key for request encryption.

(Kiuchi at 65.) As stated in the quote, the request for connection is sent “encrypted using the server-side proxy’s public key.” (*Id.*) Thus, the request for connection is sent, under the broadest reasonable interpretation, over a “virtual private network communication link.”

c) Kiuchi teaches “sending an access request message to the secure computer network address using a virtual private network communication link”

Under the broadest reasonable interpretation of the claim, Kiuchi teaches “sending an access request message to the secure computer network address using a virtual private network communication link.” Specifically, Kiuchi describes how a client-side proxy sends an encrypted request for connection to a server-side proxy. The request for connection is an “access request message,” and the server-side proxy is at a “secure computer network address.” The request for connection is sent, under the broadest reasonable interpretation, over a “virtual private network communication link.” The interpretation applied by at least one federal court provides for a “virtual private network communication link” wherever computers privately communicate with each other by encrypting traffic on insecure communications paths. (Ex. B-4 at 10.) Kiuchi’s access request message is a private communication sent in encrypted format from one proxy to another over the insecure Internet. Accordingly, Kiuchi’s access request message is sent “using a virtual private network communication link” under the broadest reasonable interpretation.

Thus, Kiuchi teaches the claim limitation.

The Examiner incorrectly concluded that Kiuchi lacked the “sending” limitation because the identified “access request message” is a request for connection, and there is no “established” connection at the time of the message:

As such, it is agreed that **Kiuchi** does not disclose "*sending an access request message...using a virtual private communication link*" because **Kiuchi** discloses that the '*access request message*' (i.e. the request for connection) occurs before a '*virtual private communication link*' (i.e. the C-HTTP) has been established and therefore cannot use the said link. (*Appendix 3(c)*) Therefore, for at least this reason, the anticipation rejection of **claims 1, 4, and 6-16** under **Kiuchi** is withdrawn.

(RAN at 5.) As shown by the quoted statement, the Examiner interprets the claim as requiring a "virtual private network communication link" to exist before the "access request message" is sent.

The Examiner's analysis is contrary to the '180 patent. Notably, the title of the '180 patent is "Method for *establishing* secure communication link between computers of virtual private network." The specification similarly provides an example process where, in the final step, "a secure VPN is established between the user's computer and the secure target site." ('180 Patent, col. 41, ll. 46-47.) These support the view that the claimed method does not require a virtual private network communication link to exist before the method steps are performed. Rather, the virtual private network communication link may be established by performing the claimed method.

And the language of claim 1 itself shows that the Examiner's analysis of the "sending" step is incorrect. Claim 1 also includes a step of "requesting ... a secure computer network address corresponding to the secure domain name." If the requester has an *already established* virtual private network communication link to the secure computer network address (as per the Examiner's analysis), then the requester would already know that address. Why would the requester send a request to obtain it?

Even if the Examiner were correct in interpreting the claims as requiring an already-established connection, **Kiuchi** still teaches the "sending" step. Specifically, **Kiuchi** describes further communications between the client-side proxy and the server-side proxy after a connection is established. The client-side proxy uses the established secure connection to send further requests to the server-side proxy, again using encryption to protect their privacy:

6) Sending C-HTTP requests to the server-side proxy (Fig. 2g)

Once the connection is established, a client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format.

(Kiuchi at 66.) Kiuchi illustrates below an example request, as it would be dispatched by the client-side proxy, to obtain a web page “sample.html” from the server “server.in.current.connection”:

```
(2)
GET "http://server.in.current.connection/
sample.html"
HTTP/1.0<CR><LF>
```

(Kiuchi at 66.) The request to access a web page is an “access request message.” Since such a request is sent only “[o]nce the connection is established” and “in encrypted form,” (Kiuchi at 66), the request is sent, under the broadest reasonable interpretation, “using a virtual private network communication link.”

Accordingly, Kiuchi teaches the “sending” step not only under the broadest reasonable interpretation, but also consistent with the Examiner’s analysis. Since this limitation was the sole basis for the Examiner’s decision to withdraw the rejection of claims 1, 17, and 33, the Board should reverse the Examiner and reinstate the rejection of these claims as anticipated by Kiuchi.

C. Issue 1: Kiuchi Anticipates Claims 6, 22, and 37

Claim 6 recites in part, “wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.” Claims 22 and 37 include a similar limitation. The Examiner relied on this limitation in her decision to withdraw the rejection of these claims as anticipated by Kiuchi. (RAN at 9.)

Kiuchi teaches that version information is transmitted in each request and response message. For example, in Kiuchi’s example messages, the version information “C-HTTP/0.7” is sent to indicate that the programs support the level of service provided by version 0.7 of the C-HTTP protocol. (See Kiuchi at 70, 71.)

The Examiner agreed that the version information indicates a “predetermined level of

service,” but stated that the version information was inserted into a request or response message, but not into a data packet as claimed:

Nonetheless, 3PR’s argument is not persuasive because it is found that **Kiuchi**’s C-HTTP Version = ‘C-Http/0.7’ is not inserted into a data packet, as claimed, but rather the C-HTTP version is transmitted as request-line or a version-line, respectively. (*Kiuchi* pg. 70 at §2.1 and pg. 71 at §2.1) Therefore, for this additional reason, the anticipation rejection of **claims 6, 22 and 37** under **Kiuchi** is withdrawn.

(RAN at 8-9.) In withdrawing the rejection, the Examiner failed to apply the broadest reasonable interpretation to the claim term “data packet.” Indeed, the Examiner failed to apply the same interpretation of “data packet” that she applied to other claims. For example, in addressing claim 8 the Examiner also stated (correctly) that “*Kiuchi*’s request and responses, which include the nonce values, read on the broadest reasonable interpretation of ‘data packet’ because these data, including the nonce value, are included in a packet (i.e. a bundle).” (RAN at 11 (emphasis added).)

Kiuchi’s request and response packets, which include the “C-HTTP/0.7” service level indication, are “data packets” under the broadest reasonable interpretation. Notably, the ’180 Patent mentions many types of packets: “TARP packets,” “data packets,” “IP packets” (’180 at 11: 29-58), “decoy packet” (’180 Patent, 16: 23), “secure synchronization request packet” (’180 Patent, 18: 20-21), “response packet” (’180 Patent, 18: 36), “ACK packet” (’180 Patent, 18: 37), “secure session initiation packet” (’180 Patent, 18: 41-42), and “SYNC_REQ packet” (’180 Patent, 30: 7-8). The claims, however, do not recite any particular type of packet, size of packet, or type of communication protocol for sending the packet; the claims merely recite “data packet.” If the Patent Owner had intended to limit the claim to only a particular form of packet, that limitation should be recited in the claims. To the contrary, there is nothing in the claims or the specification to suggest that “data packets” have such a limited definition, and thus, there is no basis for the Examiner’s statement that Kiuchi’s request or response message is not a “data packet” as recited in the claims. Under the broadest reasonable interpretation of “data packet,” the packets of data that form the C-HTTP request and the C-HTTP response are each a “data packet.” Accordingly, the version information included in the C-HTTP request and response is “at least one data value representing a predetermined level of service” inserted into “at least one

data packet.”

More generally, Kiuchi teaches that the C-HTTP request and C-HTTP response are sent over the Internet using TCP, or transmission control protocol. (Kiuchi at 67.) TCP is a standard protocol defined in Request for Comments 793 (Ex. D-6) and is “intended for use as a highly reliable host-to-host protocol between hosts in *packet-switched* computer communication networks.” (RFC793 at 1.) The standard also describes how buffers of data to be transmitted are packaged into a segment, the segment is packaged into a datagram, and the datagram is “embedded in a local network packet.” (*Id.* at 7.) From there, network switches perform further “operations to achieve the delivery of the local network packet to the destination internet module.” (*Id.* at 8.) Thus, *all communications* between Kiuchi’s client-side proxy and server-side proxy are by way of data packets, and Kiuchi’s C-HTTP version information is inserted into at least one data packet.

Kiuchi therefore teaches that “the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network” as recited in claim 6. The Board should reverse the Examiner and reinstate the rejection of claims 6, 22, and 37.

D. Issue 1: Kiuchi Anticipates Claims 8, 24, and 39

Claim 8 recites in part, “comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.” Claims 24 and 39 recite similar limitations. Kiuchi teaches this limitation through the use of nonce values included in each C-HTTP request and response.

Kiuchi discloses a “moving window of valid values” because the Nonce values of Kiuchi are values that indicate where a packet belongs in a message sequence, and the Nonce values are checked to prevent replay attacks. Kiuchi discusses an example sequence involving a number of requests and responses. (Kiuchi at 74-75.) Within those requests and responses are the Nonce values. Those Nonce values from those requests and responses are reproduced below:

<u>Request Nonce Sequence</u>	<u>Response Nonce Sequence</u>
8abd853f	ef23dc99
↓	↓
8abd8540	ef23dc9a
↓	↓
8abd8541	ef23dc9b

(See Kiuchi at 74-75.)

The Examiner found that these nonce values are not “moving” because “the differences between the nonce values are variable.” (RAN at 10.) The Examiner is incorrect. The nonce values increment by 1 on each line using ordinary hexadecimal notation.¹ In any event, the claim merely recites a “moving window,” and thus under the broadest reasonable interpretation of the claim, it does not matter how the nonce values vary from one to the next; it is enough that they are “moving.” As shown in the table above, it is clear from Kiuchi’s disclosure that the request nonce value changes with each request, and similarly the response nonce value changes with each response.

Furthermore, Kiuchi teaches that these nonce values are verified to ensure that the received values are as expected: “When the server-side proxy obtains the client-side proxy’s IP address, hostname, and public key, it authenticates the client-side proxy, *checks the integrity of the request and the request Nonce value.*” (Kiuchi at 66, emphasis added.) Thus, each expected Nonce value corresponds to a “window of valid values.”

In summary, Kiuchi teaches verifying a Nonce value to ensure the integrity of a packet and that the Nonce value changes for each packet. Thus, Kiuchi teaches “comparing a value in each data packet transmitted ... to a moving window of valid values” as recited in claim 8. The Board should reverse the Examiner’s decision and reinstate the rejection of claims 8, 24, and 39 as anticipated by Kiuchi.

E. Issues 1, 2, & 3: Dependent Claims Will Fall Together with the Independent Claims

The Examiner withdrew the rejection of various claims based solely on her decision to withdraw the rejection of independent claims 1, 17, and 33. In particular, the Examiner withdrew the rejection of:

- claims 9, 24 and 40 as anticipated by Kiuchi (RAN at 13);
- claims 12 and 28 as anticipated by Kiuchi (RAN at 15);

¹ As would be well understood by one of ordinary skill in the art, hexadecimal notation is frequently used in the computer-related arts and refers to a scheme for writing numeric values using base 16. The letters *a* through *f* correspond to the decimal (base 10) values of 10 through 15. Thus, in hexadecimal notation, $9+1=a$ and $f+1=10$.

- claims 13, 15, 29, and 31 as anticipated by Kiuchi (RAN at 16);
- claims 4, 10, 14, 20, 26, 30, and 35 as anticipated by Kiuchi (RAN at 17);
- claims 11, 27, and 41 as obvious over Kiuchi (RAN at 19);
- claims 7, 23, and 38 as obvious over Kiuchi in view of Martin (RAN at 20).

Because the Examiner withdrew these rejections based solely on the erroneous decision to withdraw the rejection of claims 1, 17, and 33, the Board should reverse the Examiner and reinstate these rejections. In other words, these claims will fall together with the independent claims.

VIII. Conclusion

Payment in the amount of \$2000.00 as required by 37 CFR 41.20(b)(2)(ii) is included with this Appeal Brief. The Director is hereby authorized to charge any additional fees or credit any fees required to Deposit Account No. 08-1394.

For the reasons provided above, Requester Cisco Systems respectfully asks the Board to reverse the decisions of the Examiner and to reinstate all of the withdrawn claim rejections. As identified in the attached Certificate of Service, a copy of the present Appeal Brief, in its entirety, is being served to the address of the attorney or agent of record.

Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: June 28, 2013
HAYNES AND BOONE, LLP
IP Section, 2323 Victory Avenue,
Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Facsimile: 214/200-0853
R-335631_1.docx

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence, all attachments, and any corresponding filing fee is being transmitted via the Electronic Filing System (EFS) Web with the United States Patent and Trademark Office on June 28, 2013.

Theresa O'Connor

IX. Claims Appendix

1. A method for accessing a secure computer network address, comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.

4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.

6. The method according to claim 4, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

7. The method according to claim 4, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

8. The method according to claim 4, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

9. The method according to claim 4, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

10. The method according to claim 1, wherein the virtual private network includes the Internet.

11. The method according to claim 1, wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.

12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.

13. The method of claim 1, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;
wherein sending the query message comprises sending the query message at the client computer;

wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access request message comprises sending the access request message at the client computer.

14. The method of claim 1, performed by a software module.

15. The method of claim 1, performed by a client computer.

16. The method of claim 2, wherein receiving the command comprises receiving the command at a client computer from a user.

17. A computer-readable storage medium, comprising:
a storage area; and
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address

corresponding to the secure domain name;

receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.

22. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

23. The computer-readable medium according to claim 20, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

24. The computer-readable medium according to claim 20, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

25. The computer-readable medium according to claim 20, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.

27. The computer-readable medium according to claim 17, wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.

28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.

29. The computer-readable medium according to claim 17, wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;
wherein sending the query message comprises sending the query message at the client computer;

wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access request message comprises sending the access request message at the client computer.

30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.

31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.

32. The computer-readable medium according to claim 18, wherein receiving the command comprises receiving the command at a client computer from a user.

33. A data processing apparatus, comprising:
a processor, and memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.

37. The apparatus of claim 35, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

38. The apparatus of claim 35, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

39. The apparatus of claim 35, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

40. The apparatus of claim 35, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

41. The apparatus of claim 33, wherein the secure domain name has a top-level domain name that includes one of scom, .snet, .sorg, .sedu, smil or .sgov.

X. Evidence Appendix

Requester does not rely on any declarations submitted under 37 C.F.R. §§ 1.30, 1.131, or 1.132.

Requester relies on the following prior art evidence. Although these references are already of record in the proceeding, in an abundance of caution vis-à-vis 37 C.F.R. § 41.67(c)(1)(ix), Requester files herewith copies of the prior art evidence. For the avoidance of confusion, Requester has labeled its exhibits consistently throughout this proceeding. Exhibits A-E were included in the Request for Reexamination on October 25, 2011; and Exhibits F-I were filed with Third Party Requester’s Comments on January 16, 2013.

<u>Exhibit</u>	<u>Document</u>	<u>Originally Filed</u>	<u>Entered</u>
A	U.S. Patent No. 7,188,180	Oct. 25, 2011	Office Action, page 2 (Sept. 19, 2012).
D-2	“Kiuchi”: Takahiro Kiuchi and Shigekoto Kaihara, “C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet,” published in the Proceedings of SNDSS 1996.	Oct. 25, 2011	Office Action, page 2 (Sept. 19, 2012).
D-4	“Martin”: David M. Martin, “A Framework for Local Anonymity in the Internet,” Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).	Oct. 25, 2011	Office Action, page 2 (Sept. 19, 2012).
D-6	“RFC 793”: Information Sciences Institute, “Transmission Control Protocol,” DARPA Internet Program Protocol Specification RFC 793 (Sept. 1981).	Oct. 25, 2011	Action Closing Prosecution, page 2 (Feb. 27, 2012).
F	Joint Claim Construction Chart for US 7,188,180, <i>VirnetX v. Cisco</i> , No. 6:10-cv-00417, Docket No. 194 (Dec. 21, 2011) (selected pages).	Jan. 16, 2013	Action Closing Prosecution, page 2 (Feb. 27, 2012).

<u>Exhibit</u>	<u>Document</u>	<u>Originally Filed</u>	<u>Entered</u>
G	U.S. Patent No. 5,706,218	Jan. 16, 2013	Action Closing Prosecution, page 2 (Feb. 27, 2012).
H	Excerpt from Microsoft Computer Dictionary, Fourth Edition	Jan. 16, 2013	Action Closing Prosecution, page 2 (Feb. 27, 2012).
I	Excerpt from <i>A First Course in Probability</i> , Sixth Edition, Sheldon Ross	Jan. 16, 2013	Action Closing Prosecution, page 2 (Feb. 27, 2012).

XI. Related Proceedings Appendix

Requester files herewith a copy of the following decisions entered in the litigations identified above in Section II. For avoidance of confusion, Requester has labeled its exhibits consistently throughout this proceeding. Exhibits A-E were included in the Request for Reexamination on October 25, 2011; and Exhibits F-I were filed with Third Party Requester's Comments on January 16, 2013.

Exhibits J, K, and L have issued during the pendency of this reexamination and are not previously of record.

<u>Exhibit</u>	<u>Document</u>
Ex. B-4	MEMORANDUM OPINION AND ORDER (regarding claim construction), <i>VirnetX Inc. v. Microsoft Corp.</i> , Case no. 6:07-cv-80 (E.D. Tex. Jul. 30, 2009).
Ex. J	FINAL JUDGMENT (regarding Apple, Inc.), <i>VirnetX Inc. v. Cisco Systems, Inc. et al.</i> , Case no. 6:10-cv-417 (E.D. Tex. Feb. 27, 2013).
Ex. K	FINAL JUDGMENT (regarding Cisco Systems, Inc.), <i>VirnetX Inc. v. Cisco Systems, Inc. et al.</i> , Case no. 6:10-cv-417 (E.D. Tex. Mar. 19, 2013).
Ex. L	MEMORANDUM OPINION AND ORDER (regarding claim construction), <i>VirnetX Inc. v. Cisco Systems, Inc. et al.</i> , Case no. 6:10-cv-417 (E.D. Tex. Apr. 25, 2012).

XII. Certificate of Service

The undersigned certifies that a copy of the THIRD PARTY REQUESTER CISCO SYSTEMS, INC.'S APPEAL BRIEF and Exhibits A, B-4, D-2, D-4, D-6, and F – L were served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

the attorneys of record for the assignee of USP 7,188,180 in accordance with 37 CFR § 1.903, on June 28, 2013.

/David L. McCombs / _____

David L. McCombs,
Registration No. 32,271

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:					
Filing Appeal Brief Inter Partes Reexam	1404	1	2000	2000	
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				2000

Electronic Acknowledgement Receipt

EFS ID:	16184045
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	28-JUN-2013
Filing Date:	25-OCT-2011
Time Stamp:	11:51:11
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2000
RAM confirmation Number	11202
Deposit Account	081394
Authorized User	MCCOMBS, DAVID L

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		Third_Party_Requesters_Appeal_Brief.pdf	364965 b125b85cbe77427ff846013a0a83b57cf3d538d1	yes	25
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Appeal Brief - Third Party Requester	1	24	
		Reexam Certificate of Service	25	25	
Warnings:					
Information:					
2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_A_pat7188180.pdf	5232014 4e7d238f27408026996276328d9327292b9e1809	no	84
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B4_VirnetX_v_Microsoft_Markman_Order.pdf	2204228 ade30f58a0e8057b360ffb22d844ebd2d77a7899	no	36
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D2_Kiuchi.pdf	971751 beaa218beb11a6cb400eb59cef039e8a7ea0da71	no	13
Warnings:					
Information:					
5	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D4_Martin.pdf	2221758 111b2303fdb7b1a5d3a339be377a1aa73ebc839b	no	15
Warnings:					
Information:					
6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D6_rfc793.pdf	2988269 c84c07f54cb9ae9e55b269f12d95def288b8355	no	90
Warnings:					
Information:					

7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_F_Joint_Claim_Construction_Excerpt.pdf	127192 d8d61c1d1750ae677c991fb37f40c06cebfc3872	no	7
Warnings:					
Information:					
8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_G_US5706218.pdf	402964 1870ba20ed4a333eac7c51ab1601f6113e1779cb	no	7
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_H_MS_Comp_Dict.pdf	988183 3c0f1df18d887fd6c9cf2051eb9807866ea587b	no	4
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_I_Probability.pdf	122722 1e49a841d776eb6f84eb55da9f6ca3dc8a5b2b57	no	5
Warnings:					
Information:					
11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX_J_FINAL_JUDGMENT_for_Apple.pdf	160007 f0dde977558d0077648769ac4dfc0a4fcc4620	no	3
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_K_FINAL_JUDGMENT_for_Cisco.pdf	143755 98a0e3f7fad5c89801ddc3d3c144f03fddde262f	no	3
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_L_VirnetX_v_Cisco_Markman_Order.pdf	439724 4f71b42cb72e40e1bdc77ce4890cc078f028d383	no	32
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	30594 d0242c91cf76ebd8c66a5960e77f0bc8a9ed16ac	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			16398126		

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 <i>Inter Partes</i> Reexamination of:)	
)	
Victor Larson et al.)	Control No.: 95/001,792
)	
U. S. Patent No. 7,188,180)	Group Art Unit: 3992
)	
Issued: March 6, 2007)	Examiner: Deandra M. Hughes
)	
For: METHOD FOR ESTABLISHING SECURE)	Confirmation No. 1972
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 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:

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: June 10, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	15996032
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Pier Douglas DeRoo/Sheryl Lewis
Filer Authorized By:	Pier Douglas DeRoo
Attorney Docket Number:	43614.100
Receipt Date:	10-JUN-2013
Filing Date:	25-OCT-2011
Time Stamp:	16:31:25
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	COS180.pdf	43735 4b181f9993e3d72d292124a6078787597661031a	no	1

Warnings:

Information:

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.: 95/001,792
)
U.S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK.)
)

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. 7,188,180 (the '180 patent), which is the subject of this proceeding, is currently at issue in the following litigation:

VirnetX Inc. and Science Applications Int'l Corp. v. Microsoft Corp.,
No. 6:13-cv-00351 (E.D. Tex.).

The '180 patent was initially at issue in the following litigation, but was later withdrawn:

VirnetX Inc. and Science Applications Int'l Corp. v. Cisco Systems, Inc., Apple Inc., Aastra USA, Inc., Aastra Technologies Ltd., NEC Corp., and NEC Corp. of America, No. 6:10-cv-00417 (E.D. Tex.).

The '180 patent was previously at issue in the following litigations, in which the parties reached a settlement agreement:

VirnetX Inc. and Science Applications Int'l Corp. v. Microsoft Corp.,
No 6:07-cv-00080 (E.D. Tex.);

VirnetX Inc. v. Microsoft Corp., No. 6:10-cv-00094 (E.D. Tex.).

The '180 patent was previously at issue in an *inter partes* reexamination proceeding filed by Microsoft Corporation on December 8, 2009 with Control No. 95/001,270.

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:	15982200
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Pier Douglas DeRoo/Beverly Green
Filer Authorized By:	Pier Douglas DeRoo
Attorney Docket Number:	43614.100
Receipt Date:	07-JUN-2013
Filing Date:	25-OCT-2011
Time Stamp:	15:45:04
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 Miscellaneous Incoming Letter	Litigation_Notice_180_Patent.pdf	68960 7490ba5bbac5f66307c19fa97228fb2ca6dd228b	no	2

Warnings:

Information:

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

Reexamination Control No.: 95/001,792	§	Attorney Docket No.: 43614.100
	§	
Patent No.: 7,188,180	§	Customer No.: 27683
	§	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	§	Real Party In Interest: Cisco Systems, Inc.
	§	
Examiner: Deandra M. Hughes	§	
	§	
Art Unit: 3992	§	Conf. No. 1972

Mail Stop: *Inter Partes* Reexamination
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

NOTICE OF APPEAL

Requester hereby provides notice under the provisions of 37 C.F.R. § 41.20 to appeal to the Patent Trial and Appeals Board with respect to all of the Examiner's decisions favorable to the patentability of the claims in reexamination, including the decisions favorable to patentability set forth in the Right of Appeal Notice mailed April 12, 2013.

More specifically, Requester intends to contest the proposed rejections for which reexamination was ordered but which are not adopted by the Examiner, including at least the following:

- Issue 1:** Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, and 39-40 are anticipated by Kiuchi.
- Issue 2:** Claims 11, 27, and 41 are rendered obvious by Kiuchi.
- Issue 3:** Claims 7, 23, and 38 are rendered obvious by Kiuchi in view of Martin.

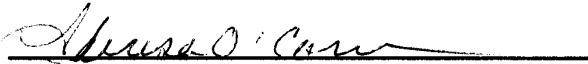
For clarity of the record, Requester notes that Claims 2, 3, 5, 18, 19, 21, 34, and 36 are not subject to reexamination. And although Requester proposed additional rejections in the Request for Reexamination, the Patent Office has not made any decision regarding those proposed rejections or the other prior art submitted with the Request. *See Belkin Int'l, Inc. v. Kappos*, 696 F.3d 1379, 1384 (Fed. Cir. 2012).

Payment in the amount of \$800.00 as required by 37 CFR 41.20(b)(1) is included with this Notice. The Director is hereby authorized to charge any additional fees required to Deposit Account No. 08-1394.

Respectfully submitted this 1st day of May, 2013,

/David L. McCombs/
David L. McCombs
USPTO Reg. No. 32,271

HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Facsimile: 214/200-0853
Docket No. 43614.100

<p style="text-align: center;">CERTIFICATE OF TRANSMISSION</p> <p>I hereby certify that this correspondence, all attachments, and any corresponding filing fee is being transmitted via the Electronic Filing System (EFS) Web with the United States Patent and Trademark Office on May 1, 2013.</p> <p style="text-align: center;"> _____ Theresa O'Connor</p>

CERTIFICATE OF SERVICE

Pursuant to M.P.E.P. § 2683 and 37 C.F.R. §§ 1.248 and 1.983(b)(3), the undersigned attorney for Appellants certifies that a copy of the NOTICE OF APPEAL was served, via United States Postal Service First Class Mail, on May 1, 2013 on the counsel for Patent Owner at the following address:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

/David L. McCombs/
David L. McCombs

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:	15660124
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	01-MAY-2013
Filing Date:	25-OCT-2011
Time Stamp:	11:06:48
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	10138
Deposit Account	081394
Authorized User	MCCOMBS, DAVID L

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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		3PR_Notice_of_Appeal.pdf	79093 b75fd9fdb4d8cf7de178c3ab0c0df69617d91485	yes	3
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Notice of Appeal - Requester	1	2	
		Reexam Certificate of Service	3	3	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30566 f6ae27c15e55de21cb5da081019616833c4a1e2f	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			109659		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					



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.
-----------------	-------------	----------------------	---------------------	------------------

95/001,792	10/25/2011	7,188,180	43614.100	1972
------------	------------	-----------	-----------	------

22852 7590 04/12/2013
 FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
 LLP
 901 NEW YORK AVENUE, NW
 WASHINGTON, DC 20001-4413

EXAMINER

HUGHES, DEANDRA M

ART UNIT	PAPER NUMBER
----------	--------------

3992

MAIL DATE	DELIVERY MODE
-----------	---------------

04/12/2013	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 <i>Inter Partes</i> Reexamination	Control No.	Patent Under Reexamination	
	95/001,792	7,188,180	
	Examiner	Art Unit	
	Deandra M. Hughes	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219

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.

Right of Appeal Notice (37 CFR 1.953)	Control No.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	Deandra M. Hughes	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 19 December, 2012
 Third Party(ies) on 16 January, 2012

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 1,4,6-17,20,22-33,35 and 37-41 are subject to reexamination.
- 1b. Claims _____ are not subject to reexamination.
2. Claims _____ have been cancelled.
3. Claims 1,4,6-17,20,22-33,35 and 37-41 are confirmed. [Unamended patent claims].
4. Claims _____ are patentable. [Amended or new claims].
5. Claims _____ 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. _____

INTER PARTES REEXAMINATION RIGHT OF APPEAL NOTICE

1. This is a right of appeal notice (“RAN”) in the *inter partes* reexamination of USP 7,188,180. (“**180 patent**”) The action closing prosecution (“ACP”) was mailed on February 27, 2013. Patent Owner’s (“PO”) comments under 37 CFR 1.951(a) have not been received. As such, RAN is proper under 37 CFR 1.953(a) and the reasons for confirmation set forth in the ACP are maintained here.

Evidence Cited in this Action

2. The evidence is cited in this action:
- (A) Kiuchi et al. “*The Development of a Secure, Closed HTTP-based Network on the Internet*”, 1996. (“**Kiuchi**”)
 - (B) Martin, David M. “*A Framework for Local Anonymity in the Internet*”, February 21, 1998. (“**Martin**”)
 - (C) RFC973: Information Sciences Institute, “Transmission Control Protocol”. DARPA Internet Program Protocol. Sept. 1981. (“**RFC973**”)
 - (D) Declaration of Dr. Angelos D. Keromytis, Ph.D. executed Dec. 16, 2012. (“**Keromytis Declaration**”)
 - (E) Declaration of Dr. Robert Dunham Short III, Ph.D. executed Dec. 18, 2012. (“**Short Declaration**”)

[The remainder of this page is intentionally left blank.]

Response to PO's Remarks and 3PR's Comments

I. *Summary of Kiuchi*

Kiuchi discloses "C-HTTP" which provides secure HTTP communications within a closed group of institutions on the internet, where each member is protected by its own firewall. (*Abstract*) **Kiuchi** discloses that these C-HTTP-based communications are made possible by three components: (1) a client-side proxy, (2) a server-side proxy, and (3) a C-HTTP name server. (*Id.*) The client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol, while communications between a user agent and client-side proxy or an origin server and server-side proxy are performed using HTTP/1.0. (*Id.*) In a C-HTTP-based network, instead of DNS, a C-HTTP-based secure, encrypted name, and certification service is used. (*Id.*)

II. *Claim 1: "sending an access request message to the secure computer network address using a virtual private network communication link."*

As to this claim limitation, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi's** disclosed "request for connection to the server-side proxy" of *Appendix 3(c)* reads on the claimed "access request message" and the disclosed "C-HTTP connection between a client-side proxy and a server-side proxy" reads on the claimed "virtual private network communication link". (*Claim Charts, Exhibit E-2, pg. 13-16*)

PO argues **Kiuchi's** claimed "request for connection" of *Appendix 3(c)* is sent before any C-HTTP connection is established, and accordingly **Kiuchi** fails to disclose "sending an access request message...using a virtual private communication link" because the "access request message" (i.e., request for connection) cannot use a

Art Unit: 3992

virtual private communication link (i.e., the C-HTTP connection) that has not yet been established. (*Remarks, pg. 6; emphasis added*)

PO also provides the **Keromytis Declaration**, which makes the following statement as to **Kiuchi** (§23):

23. A person of ordinary skill in the art at the time of the invention would also have understood that the mere two steps of (1) contacting a name server to obtain a server-side proxy's public key, and then (2) using that public key to encrypt a request for connection, do not thereby create a "virtual private network communication link." This is because, in this situation, no "link" exists at all between the client-side and server-side proxies at the time the "request for connection" is sent. Rather, there is only a one-way communication sent as part of *setting up* the C-HTTP connection. (*Kiuchi 64-65.*)

3PR responds that when the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, the client-side proxy sends a request for connection to the server-side proxy's public key. (*Comments, pg. 2 lines 3-6 citing Kiuchi at p.65*)

Upon examination of **Kiuchi**, it is found the claim term 'private' modifies the claim term 'network' and as such, **Kiuchi** must teach the 'privacy' of the 'network' and not just the privacy of the 'communication link' to anticipate the claims.

Second, it is found that **Kiuchi** discusses a 'virtual network' only once, which is reproduced below.

5. Concluding remarks

Although C-HTTP is primarily developed for use in the medical field, it can be used in other areas. Using C-HTTP, a closed HTTP-based virtual network can be constructed for closed groups, for example, the headquarters and branches of a given corporation. This kind of usage may not fit with the spirit of the Internet, but if resources which might otherwise be invested in private circuits are channeled into the Internet, it will contribute to its further development.

Third, it is found that this disclosure by **Kiuchi** that "[u]sing C-HTTP, a closed HTTP-based virtual network can be constructed for closed groups" applies to the C-HTTP that is established *in response* to a "request for connection to the server-side proxy" of *Appendix 3(c)* because the request for connection occurs *before* the C-HTTP (i.e. the virtual private network communication link) is established.

As such, it is agreed that **Kiuchi** does not disclose "*sending an access request message...using a virtual private communication link*" because **Kiuchi** discloses that the '*access request message*' (i.e. the request for connection) occurs before a '*virtual private communication link*' (i.e. the C-HTTP) has been established and therefore cannot use the said link. (*Appendix 3(c)*) Therefore, for at least this reason, the anticipation rejection of **claims 1, 4, and 6-16** under **Kiuchi** is withdrawn.

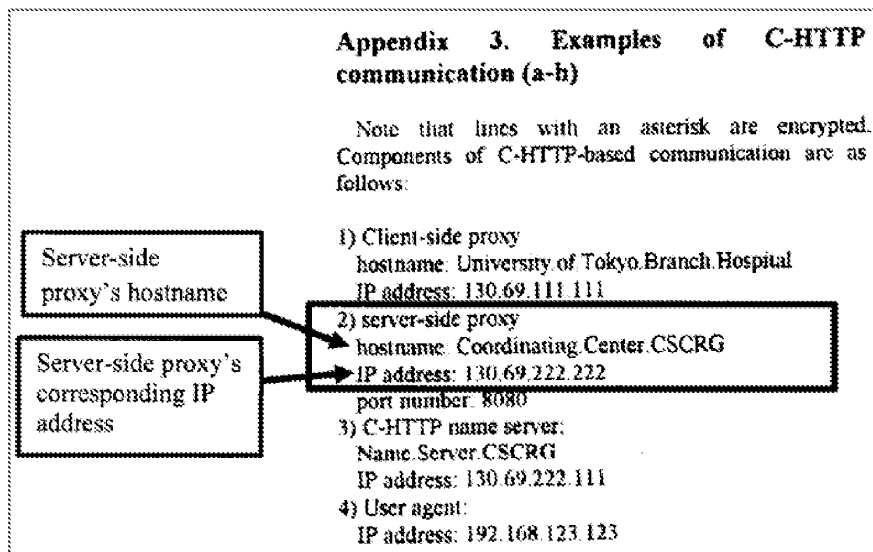
III. *Claim 1: "the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name"*

As to this claim limitation, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi's** disclosed `Coordinating.Center.CSCRG` reads on the claimed "*secure domain name*" and the disclosed secure server-side proxy IP address reads on the claimed "*secure computer network address*". (*Claim Charts, Exhibit E-2, pgs. 9-10*)

PO argues **Kiuchi's** URL (i.e. the claimed 'secure domain name') does not correspond to the server-side proxy, but rather the resource itself located on an origin server. (*Remarks, pg. 8, lines 3-5*) The **Keromytis Declaration** does not address this claim limitation.

3PR responds that PO ignores the example in *Appendix 3(a) and 3(b)* of **Kiuchi**, where **Kiuchi** teaches an embodiment in which the IP address returned by the name server is the IP address that directly corresponds to the hostname contained in the query message. (*Comments, pg. 4, 1st ¶*)

Upon examination of **Kiuchi**, it is found that **Kiuchi's Appendix 3: Examples of C-HTTP Communication (a-h)**, which is reproduced below with 3PR's annotations, discloses that the claimed "secure domain name" (i.e., `Coordinating.Center.CSCRG`) corresponds to the claimed "secure computer network address" (i.e., IP address: `130.69.222.222`). As such, PO's argument is not persuasive.



However, for the reason that **Kiuchi** does not disclose "*sending an access request message...using a virtual private communication link*", as discussed above, the anticipation rejection of **claim 1** under **Kiuchi** is withdrawn.

Art Unit: 3992

IV. Claims 17 and 33

PO incorporates by reference the arguments traversing the rejection of **claim 1** over **Kiuchi**. As such, the response to these arguments, as set forth above, is incorporated here. Therefore, for at least the reason incorporated here, the anticipation rejection of **claims 17, 20, 22-33, 35, and 37-41** under **Kiuchi** is withdrawn.

V. Claims 6, 22, and 37

As to the claim limitation "*the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network*", the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that, *inter alia*, the value in the allegedly inherent 'type of service field' in the TCP/IP session disclosed by **Kiuchi** reads on the claimed 'data value'. (*Claim Charts, Exhibit E-2, pgs. 21-22 citing RFC 793 to support inherency*)

PO argues **Kiuchi** does not specifically or inherently disclose this limitation because the evidence (*i.e.*, *RFC 793 at p. 12*) does not support the conclusion that **Kiuchi's** C-HTTP system would necessarily insert into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network. (*Remarks, pg. 9, last ¶*)

PO also provides the **Keromytis Declaration**, which makes the following statement as to **Kiuchi** (*¶27*):

Art Unit: 3992

27. *Kiuchi* simply does not describe any nexus between RFC 793's "type of service" fields and the alleged virtual private network (i.e., the C-HTTP connection) or a predetermined level of service associated with a C-HTTP connection. Thus, a person of ordinary skill would not have understood *Kiuchi*'s C-HTTP connection to be "based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network." Accordingly, a person of ordinary skill would not have understood *Kiuchi* to show, either expressly or inherently, that "the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network," as recited in claims 6, 22, and 37.

3PR responds that **Kiuchi** discloses this limitation because **Kiuchi** discloses inserting version information (e.g., C-HTTP Version = 'C-Http/0.7') in the request and into the response. (*Comments, pg. 6, last ¶, citing Kiuchi at 70, 71*) 3PR argues the C-HTTP version value inserted into the request and the response defines the "version of C-HTTP name service protocol" being used. (*Comments, pg. 6, last ¶, citing Kiuchi at 72*) Further, 3PR states the version of the name service protocol is a data value representing a predetermined level of service. (*Comments, pg. 6, last ¶*) Accordingly, 3PR argues that **Kiuchi** discloses "the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network" because **Kiuchi** inserts version information defining the name service into each request and response, (*Comments, pg. 6, 1st ¶*)

Upon examination of **Kiuchi**, it is found that 3PR's argument as to 'inserting version information' was not presented in the request and claim charts (*see Exhibit E-2, pgs. 21-22, 35, and 37*). As such, PO has not yet had an opportunity to address this materially different and newly presented version of the anticipation rejection of **claims 6, 22, and 37** under **Kiuchi**. Nonetheless, 3PR's argument is not persuasive because it is

Art Unit: 3992

found that **Kiuchi's** C-HTTP Version = 'C-Http/0.7' is not inserted into a data packet, as claimed, but rather the C-HTTP version is transmitted as request-line or a version-line, respectively. (*Kiuchi pg. 70 at §2.1 and pg. 71 at §2.1*) Therefore, for this additional reason, the anticipation rejection of **claims 6, 22 and 37** under **Kiuchi** is withdrawn.

VI. Claims 8, 24, and 39

As to the claim limitation "*the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values*", the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that, *inter alia*, **Kiuchi's** disclosed nonce values reads on the claimed "*value in each data packet*". (*Claim Charts, Exhibit E-2, pgs. 22-25*)

PO argues **Kiuchi** does not anticipate these claims because they do not specifically or inherently disclose this limitation because **Kiuchi** does not disclose (1) comparing the nonce header field to a 'moving window of values' or (2) the nonce values are inserted into each data packet. (*Remarks, pg. 10*)

As to PO's first argument, PO argues **Kiuchi** does not disclose this claim limitation because **Kiuchi** at *pg. 74*, which discusses incrementing the Request-Nonce value, teaches that different types of requests might contain different nonce values. (*Remarks, pg. 10, 2nd ¶*) PO argues that this disclosure does not, however, teach that **Kiuchi's** nonce values are compared to a "*moving window of valid values*", as claimed. (*Id.*) Further, PO argues, there are many ways the values of **Kiuchi's** nonce header field could be checked without comparing them to a moving window of valid values. (*Id.*) PO

Art Unit: 3992

provides the **Keromytis Declaration** as opinion evidence to support PO's arguments.

(¶¶29-30)

3PR responds that PO's arguments contradict the specification of the '**180 patent**, which allegedly defines a "moving window of values" as "1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence." (*Comments, pg. 8 last ¶ citing '180 patent, col.11:59-61*)

Upon examination of the '**180 patent**, it is found that *col.11:59-61* defines a 'window sequence number' but does not define a 'moving window of values', as argued by PO. This portion of the '**180 patent** is reproduced below:

In a preferred embodiment, the TARP headers D_T are IP headers with added data providing the following information 55 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.

As such, for the reason that 3PR's argument is premised on an erroneous claim construction, i.e., that the claim limitation 'moving window of values' is defined as the disclosed 'window sequence number', this argument is not persuasive.

Further, assuming *arguendo*, that claim construction of 'moving window of values' is as 3PR argues, then this argument is not persuasive because it is found that the patterns 3PR allege are 'incremented' are merely different because '853f...8540...8541' and 'c99...c9a..c9b' do not suggest 'incrementation' because the differences between the nonce values are variable. The chart 3PR produced to support the 'incrementation' argument is reproduced below. (*Comments, pg. 8*)

Art Unit: 3992

Request-Nonce	Response-Nonce
8abd853f	ef23dc99
8abd8540	ef23dc9a
8abd8541	ef23dc9b

As to PO's second argument, PO argues **Kiuchi** does not disclose that the nonce value is inserted into each data packet because **Kiuchi** discloses that the C-HTTP requests and responses, and not the data packets, contain the nonce values. (*Remarks, pg. 10, last ¶*) PO also provides the **Keromytis Declaration** as opinion evidence to support PO's arguments. (*¶30*)

3PR responds that PO is importing limitations from the specification into the claims and that the specification of the '**180 patent** mentions many types of 'data packets' and does not limit them to the 'IP packet' or the 'ACK packet'. (*Comments, pg. 9, 2nd ¶*)

Upon examination of **Kiuchi**, it is found that **Kiuchi**'s request and responses, which include the nonce values, read on the broadest reasonable interpretation of 'data packet' because these data, including the nonce value, are included in a packet (i.e. a bundle). As such, PO's second argument is not persuasive.

Nonetheless, for the reason that it is agreed that **Kiuchi** does not disclose the claimed "moving window of values", the anticipation rejection of **claims 8, 24, and 39** under **Kiuchi** is withdrawn.

Art Unit: 3992

VII. Claims 9, 25, and 40

As to the claim limitation "*the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields*", the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi**'s disclosed connection ID field reads on the claimed "*discriminator field*". (*Claim Charts, Exhibit E-2, pgs. 22-25*)

PO argues **Kiuchi** does not specifically or inherently disclose this limitation because **Kiuchi**'s disclosed 'connection ID' is not inserted into a header of each data packet and **Kiuchi**'s virtual private network is not disclosed as *based on a comparison* of the disclosed 'connection ID'. (*Remarks, pg. 11*)

As to PO's first argument, PO argues **Kiuchi**'s 'connection ID' (i.e. the claimed 'discriminator field'), constitutes a portion of a resource name and is not "*in a header of each data packet*" as claimed.

3PR responds that PO is importing limitations from the specification into the claims and that the specification of the '**180 patent** mentions many types of 'data packets' and does not limit them to the 'IP packet' or the 'ACK packet'. (*Comments, pg. 10, 1st ¶*)

Upon examination of **Kiuchi**, it is found that the disclosed general-header contains the 'connection ID'. (*pg. 71, §1.3 item 7*) As such, PO's argument that **Kiuchi**'s 'connection ID' (i.e., the claimed 'discriminator field') is not "*in a header of each data*

Art Unit: 3992

packet", as claimed, is not persuasive because it is found that **Kiuchi**'s 'connection ID' is disclosed as part of the general header.

As to PO's second argument, PO argues that virtual private network is not disclosed as *based on a comparison* of the disclosed 'connection ID' (i.e., the claimed 'discriminator field') because **Kiuchi**'s C-HTTP, if anything, is based on a timer, not on a 'connection ID'. PO also provides the opinion evidence of the **Keromytis Declaration** to support his argument. (§33)

3PR responds that **Kiuchi** discloses this limitation because **Kiuchi** discloses that the 'connection ID' is compared against a table of current connections, and if the 'connection ID' is not found, then the connection is disconnected. (*Comments, pg. 10, 2nd ¶, citing Kiuchi at 65*)

Upon examination of **Kiuchi**, it is found the 'connection ID' is stripped from the original resource name and then the original name is forwarded to the server. (*Kiuchi at 65, col.1, 1st ¶*) It is also found that when the 'connection ID' is not found in the current connection table in the client-side proxy, the current connection is disconnected. (*Id.*) As such, PO's argument that the 'connection ID' is not compared to a table of valid discriminator fields is not persuasive because the 'connection ID' (i.e., the claimed '*discriminator field*') is disclosed as being compared to a table of current connections (i.e., the claimed '*table of valid discriminator fields*'). However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1, 17, and 33**, the anticipation rejection of **claims 9, 25, and 40** under **Kiuchi** is withdrawn.

Art Unit: 3992

VIII. Claims 12 and 28

As to this claim limitation, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi**'s requested connection information, including a connection ID and a second symmetric data exchange key, are provided by the server-side proxy. (*Claim Charts, Exhibit E-2, pg. 28*) As such, the rejection argues that the disclosed 'connection information' reads on the claimed '*requested information*' and the disclosed 'server-side proxy' reads on the claimed '*secure computer network address*'.

PO argues **Kiuchi** does not disclose that "*the access request message contains a request for information stored at the secure network address*" because **Kiuchi** discloses that the connection ID and symmetric data exchange key are not stored at the secure computer network address, as recited in the claims, but rather are newly generated after the server-side proxy receives information regarding the client-side proxy from the C-HTTP name server. (*Remarks, pg. 12*) PO also provides the **Keromytis Declaration** as opinion evidence to support this argument. (§35)

3PR responds the connection ID (e.g. the information requested) is generated then stored at the secure computer network address (e.g., the server-side proxy), because **Kiuchi** teaches the server-side proxy needs to delete the connection ID after the connection is closed (i.e., in order for it to be deleted, the connection ID must have first been stored). (*Comments, pg. 11, 2nd ¶*)

Upon examination of **Kiuchi**, it is found that the response from the server-side proxy indicating that the connection has been established includes the server-side-

Art Unit: 3992

proxy-IP address (130.69.222.222) and the server-side proxy name (i.e.

Coordinating.Center.CSCRG). (pg. 74, section f) As such, it is agreed that the disclosed 'connection information' reads on the claimed '*requested information*' and the disclosed 'server-side proxy' reads on the claimed '*secure computer network address*'.

However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1 and 17**, the anticipation rejection of **claims 12 and 28** under **Kiuchi** is withdrawn.

IX. Claims 13, 15, 29, and 31

As to these claims, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues, *inter alia*, that **Kiuchi**'s disclosed 'client-side proxy' reads on the claimed 'client computer'.

(*Claim Charts, Exhibit E-2, pg. 29*)

PO argues that the client-side proxy does not read on the claimed 'client computer' because **Kiuchi** clearly distinguishes between clients and client-side proxies. (*Remarks, pg. 12*) According to PO, **Kiuchi** describes 'user agents' as entities with a firewall, while explaining that the client-side proxy resides on the firewall of an institution. (*Remarks, pg. 12, 3rd ¶ citing Kiuchi at 64*)

PO also provides the **Keromytis Declaration** as opinion evidence stating that a person of ordinary skill at the time of the invention would have been readily capable of distinguishing, as **Kiuchi** does, between client computers within an institutional firewall (e.g. a nurse's or doctor's PC in a hospital) and a client computer residing on an institutional firewall (e.g. a client-side proxy). (*¶38*)

3PR responds that **Kiuchi** teaches a user agent that communicates with a client-side proxy. (*Comments, pg. 12, 3rd ¶*) According to 3PR, a user enters a hostname into the user agent (e.g., a nurse's PC in a hospital), which sends the hostname to the client-side proxy. (*Id.*) Accordingly, 3PR argues, the client-side proxy receives the hostname and the hostname was from the user. (*Id.*) Thus, 3PR concludes, **Kiuchi** discloses the method occurring at and being performed by the client computer. (*Id.*)

In response to PO's argument that **Kiuchi**'s 'user agent' and 'client-side proxy' do not read on the claimed 'user' and 'client computer', respectively, because **Kiuchi** describes 'user agents' as within a firewall, while explaining that the client-side proxy resides on the firewall of the institution, it is noted that the features upon which PO relies (i.e., 'within a firewall' or 'on the firewall') are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As such, PO's argument is not persuasive. However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1, 17, and 33**, the anticipation rejection of **claims 13, 15, 29, and 31** under **Kiuchi** is withdrawn.

X. Claims 16 and 32

As to **claims 16 and 32**, it is agreed that the rejection of these claims is improper for the reason that **claims 16 and 32** depend upon claims **claims 2 and 18**, respectively, for which no RLP was found. (*see Order at 10-11*) Accordingly, the rejection of **claims 16 and 32** is withdrawn.

Art Unit: 3992

XI. Claims 4, 10, 14, 20, 26, 30, and 35

PO incorporates by reference the arguments traversing the rejection of **claims 1, 17, and 33** over **Kiuchi**. As such, the response to these arguments, as set forth above, is incorporated here. Therefore, for at least the reason incorporated here, the anticipation rejection of **claims 4, 10, 14, 20, 26, 30, and 35** under **Kiuchi** is withdrawn.

XII. Claims 11, 27, and 41

As to these claims, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues, *inter alia*, that the claims are obvious over **Kiuchi** because adding an 's' to indicate a secure domain to conventional domain names such as .com, .net, .org, .edu, .mil, or .gov is a design choice within the knowledge and skill in the art. (*Claim Charts, Exhibit E-2, pgs. 51-52*)

First, PO argues that the request and claim charts fail to provide the requisite articulated reasoning to support the rejection. (*Remarks, pg. 13*)

3PR responds that rearranging letters is a mere design choice. (*Comments, pg. 13*)

Upon examination, it is found that the request and claim charts, as explained in the Petition Decision (mailed 9/26/2012, pg. 14) provide a reasonable rationale for modifying **Kiuchi** because one of ordinary skill in this art would know that the added letter 's' stands for 'security'. As such, PO's argument that the rejection does not set forth the requisite 'articulated reasoning' is not persuasive because the rationale for the design choice is that it is known in the art that 's' stands for 'security'.

Second, PO argues that **Kiuchi's** taught domain names does not disclose or suggest succinctly modifying a top-level domain name to denote security; rather, PO argues, **Kiuchi's** allegedly lengthy and unwieldy domain names suggests the exact opposite. (*Remarks*, pg. 14, 2nd ¶)

3PR responds that PO is attempting to import limitations from the specification in the claims because the claims recite nothing about 'denoting security'. (*Comments*, pg. 13, 4th ¶)

Upon examination, it is found that PO's argument is not persuasive. In response to PO's argument that there is no teaching, suggestion, or motivation in **Kiuchi** that makes obvious the claim limitation, the examiner recognizes that obviousness may be established by modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

In this case, **Kiuchi** discloses the 'user agent to client-side proxy' and the 'server-side proxy to origin server' are HTTP/1.0 connections. (pg. 64, §2.1) It is well-known that HTTP/1.0 connections use conventional top-level domain names such as .com, .net, .org, .edu, .mil, or .gov. Further, it is well-known to one of ordinary skill in the art that modifying a conventional domain name with an 's' denotes security. As such, **Kiuchi** as modified by knowledge generally available in the art, i.e. HTTP/1.0

Art Unit: 3992

connections use conventional top-level domain names such as .com, .net, .org, .edu, .mil, or .gov and that 's' denotes security, makes obvious the claim limitations. As such, PO's arguments are not persuasive. However, for the reason that it is agreed that **Kiuchi** does not anticipate base claims 1, 17, and 33, the rejection of claims 11, 27, and 41 as obvious over **Kiuchi** in view of **Martin** is withdrawn.

XIII. Claims 7, 23, and 38

As to these claims, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues, *inter alia*, that although **Kiuchi** does not disclose this limitation, **Martin** teaches an IP hopping scheme because "[c]hoosing one of the source addresses 'at random' shows establishing the virtual private network communication link through pseudo randomly changing computer network addresses as recited by the claim." (*Claim Charts, Exhibit E-2, pgs. 48-50 citing Martin at pg. 9*)

PO argues that 3PR's tangential assertion that **Martin** describes choosing one of the source addresses at random, does not teach the claimed "*pseudo-randomly changing network addresses in packets, let alone a network address hopping regime that is used to pseudo-randomly change network addresses in packets.*" (*Remarks, pg. 15*)

3PR responds that "[r]andomly using different network addresses for each connection as taught by the combination of **Kiuchi** and **Martin** teaches that the source and destination network addresses in the packets transiting the virtual private network randomly change". (*Comments, pg. 15*)

Upon examination, it is found that **Martin** teaches the following (pg. 9):

4.4 Indirect Connection Addressing

Indirect addressing is straightforward but expensive. Let A_{IP} be the set of anonymous IP addresses in the lanon. $PORT = \{0, 1, \dots, 2^{16} - 1\}$ be the set of possible port numbers, and $A_{TCP} = A_{IP} \times PORT$ be the set of all possible TCP endpoint connection identifiers. Each such identifier is called an *anonymous TCP address*. A lanon client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random subject to lanon uniqueness and application-specific constraints.

Randomly choosing the source label hides the node's identity from external (and internal) observers. Later,

It is found that **Martin's** A_{TCP} , which is disclosed as the set of all possible TCP endpoint connection identifiers, reads on the claimed 'computer network addresses'. Further, **Martin** teaches a lanon client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random. As such, it is found that **Martin** teaches the claimed "*computer network address hopping regime*" because **Martin** teaches selecting its source address/port pair from A_{TCP} at random. Therefore, PO's arguments are not persuasive. However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1, 17, and 33**, the rejection of **claims 7, 23, and 38** as obvious over **Kiuchi** in view of **Martin** is withdrawn.

XIV. Secondary Considerations of Obviousness

"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 and therefore the examiner must determine whether there is a nexus between the merits of the claimed invention and the evidence of secondary considerations." MPEP §716.01(b)

1. Long Felt Need

As to the evidence of long felt need for the claim language pertaining to “receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link”, PO provides the **Short Declaration** (§§3-8).

The first example of long felt need provided by the **Short Declaration** (§§4-5) lacks the requisite nexus with the claim language because the evidence pertaining to the DARPA programs 'Information Assurance' and 'Dynamic Coalitions' identifies a general need for creating secure groups rapidly but does not identify the long felt need for “receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link”, as claimed. More importantly, the evidence lacks the requisite nexus because it does not discuss ‘secure domain name services’, ‘secure computer network address’, ‘access request messages’, or a ‘virtual private communication link’.

The second example regarding In-Q-Tel's willingness to enter into a relationship with SAIC (the original assignee of the application that led to the ‘**180 patent**’) for the development of the claimed technology lacks the requisite nexus with the said claim limitation because In-Q-Tel's willingness to enter into a relationship with SAIC may be due to other factors such as SAIC's size and reputation. (see **Short Declaration** §6)

Art Unit: 3992

More importantly, the evidence lacks the requisite nexus because it does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

As to the third example, the evidence of long felt need provided by the **Short Declaration** (§§7-11) lacks the requisite nexus with the claim limitation "*receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link*" because the evidence pertains to a general need for a secure VPN but does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

As such, the evidence of the long felt need provided by the **Short Declaration** is given very little weight because it lacks the requisite nexus with the claimed language.

2. Commercial Success

The **Short Declaration** provides evidence of SafeNet's portfolio license that includes the '**180 patent** and VirnetX's license agreement of \$200M as evidence of commercial success. (§12) This evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation "*receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link*" because the commercial success could be due to any number of market factors

Art Unit: 3992

including superior business acumen or marketing. More importantly, the evidence lacks the requisite nexus because it does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link' .

3. Skepticism

The **Short Declaration** provides evidence that the claimed invention was met with skepticism by others in the art before the inventor's work because Dr. Short argues that 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. (§§13-15) This evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation "*receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link*" because the evidence pertains to skepticism of an easy-to-set-up secure VPN connection but does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

4. Praise

The **Short Declaration** provides evidence that the claimed invention was met with praise by others because of the extensive licensing of the patented technology by Safenet, Microsoft, Aastra, Mitel, and NEC . (§§16) This evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation "*receiving*

Art Unit: 3992

from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link" because the extensive licensing could have been motivated by a desire to avoid the costs of litigation and not by respect for the non-obviousness of the invention. More importantly, the evidence lacks the requisite nexus because it does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

[The remainder of this page is intentionally left blank.]

Reasons for Confirming the Claims as Patentable

3. Independent **claims 1, 17, and 33** are confirmed as patentable over **Kiuchi**, alone or in combination, because **Kiuchi** does not disclose or make obvious “*sending an access request message to the secure computer network address using a virtual private network communication link*” in combination with the other limitations of the claims.

It is found that **Kiuchi** does not disclose or make obvious this claim limitation because the disclosed 'request for connection' of *Appendix 3(c)* (i.e., the claimed "access request message") is sent before the C-HTTP (i.e., the claimed "virtual private network communication link") and as such, the disclosed 'request for connection' does not use the C-HTTP (i.e. the claimed “virtual private network link”), as claimed, because no link exists at all between the disclosed client-side and server-side proxies at the time the ‘request for connection’ is sent. As such, the rejections over **Kiuchi** as set forth in the request and claim charts, are withdrawn and the claims are confirmed as patentable over **Kiuchi**. Further, **claims 4, 6-16, 20, 22-32, 35, and 37-41** are confirmed as patentable for at least the reason that they are dependent upon confirmed based **claims 1, 17, and 33**.

[The remainder of this page is intentionally left blank.]

Conclusion

4. **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.
5. 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).
6. 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).
7. 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**

Art Unit: 3992

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).

8. 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.

9. 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.

10. **All** correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: 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

11. 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.

12. Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties 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).

13. 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 concurrent proceeding, involving this patent 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 throughout the course of this reexamination proceeding. See MPEP §2686 and 2686.04.

14. Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central

Control Number: 95/001,792

Page 29

Art Unit: 3992

Reexamination Unit at telephone number (571) 272-7705.

Signed: /Deandra M. Hughes/
Reexamination Specialist, AU 3992


Conferees:

/Christina Y. Leung/

Primary Examiner, Art Unit 3992

/Sudhanshu C Pathak/

Supervisory Patent Examiner, Art Unit 3992

Reexamination 	Application/Control No. 95001792	Applicant(s)/Patent Under Reexamination 7,188,180
	Certificate Date	Certificate Number

Requester Correspondence Address:	<input type="checkbox"/> Patent Owner	<input checked="" type="checkbox"/> Third Party
David L. McCombs HAYNES and BOONE LLP 2323 Victory Avenue, Suite 700 Dallas, TX 75219		

LITIGATION REVIEW <input checked="" type="checkbox"/>	DMH (examiner initials)	08/25/2012 (date)
Case Name		Director Initials
Virnetx v. Cisco et al. 6:10cv417 (OPEN)		/SP/ for IY
Virnetx v. Microsoft 6:10cv94 (CLOSED)		
VirnetX v. Microsoft 6:07cv0080		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

--	--

Receipt date: 09/20/2012

RECEIVED



SEP 20 2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO		Complete if Known	
CENTRAL REEXAMINATION UNIT INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>		Control Number	95/001,792
		Filing Date	December 25, 2011
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Deandra M. Hughes
Sheet	1	of	52
		Attorney Docket Number	11798.0005

U.S. PATENTS						
Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code (if known)	MM-DD-YYYY		
		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	2	of	52	<i>Attorney Docket Number</i>	11798.0005

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)			
		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number		95/001,792
				Filing Date		December 25, 2011
				First Named Inventor		Victor Larson
				Art Unit		3992
				Examiner Name		Deandra M. Hughes
Sheet	3	of	52	Attorney Docket Number		11798.0005

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		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number		95/001,792
				Filing Date		December 25, 2011
				First Named Inventor		Victor Larson
				Art Unit		3992
				Examiner Name		Deandra M. Hughes
Sheet	4	of	52	Attorney Docket Number		11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	5	of	52	Attorney Docket Number	11798.0005

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)			
		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	6	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>(if known)</i>			
		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449/APTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	7	of	52	<i>Attorney Docket Number</i>	11798.0005

PUBLISHED U.S. PATENT APPLICATIONS						
Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code (if known)	MM-DD-YYYY		
		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
				<i>Attorney Docket Number</i>	11798.0005
Sheet	8	of	52		

FOREIGN PATENT DOCUMENTS							
Tab	Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Translation
			Country Code Number Kind Code <i>(if known)</i>				
		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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	9	of	52	<i>Attorney Docket Number</i>	11798.0005

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 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.	
	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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	10	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation 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 Invalidation 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 Invalidation 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, <i>Personal Mobility For Multimedia Services In The Internet</i> , Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., <i>Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet</i> (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, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	11	of	52	Attorney Docket Number	11798.0005

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, <i>The AltaVista Tunnel: Using the Internet to Extend Corporate Networks</i> , 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). (Goldschlag I, Onion Routing)	
	D55	Microsoft Corp., <i>Installing Configuring and Using PPTP with Microsoft Clients and Servers</i> (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., <i>IP Security for Microsoft Windows NT Server 5.0</i> (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., <i>Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services</i> (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., <i>Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead</i> (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., <i>Understanding Point-to-Point Tunneling Protocol PPTP</i> (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et al., <i>Protecting a Private Network: The AltaVista Firewall</i> , Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy <i>Implementation of Virtual Private Networks (VPNs) with IPSecurity</i> , <draft-ieff-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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO			Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			<i>Control Number</i>	95/001,792	
			<i>Filing Date</i>	December 25, 2011	
			<i>First Named Inventor</i>	Victor Larson	
			<i>Art Unit</i>	3992	
			<i>Examiner Name</i>	Deandra M. Hughes	
Sheet	12	of	52	<i>Attorney Docket Number</i>	11798.0005

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 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., <i>Virtual Private Networking An Overview</i> (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., <i>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</i> (1998) (available at http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpfrue). (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, et 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	13	of	52	Attorney Docket Number	11798.0005

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., <i>Company Focuses on Quality and Customer Feedback</i> (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, <i>Domain Name System Security Extensions</i> , 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, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. <i>Virtual Private Networks</i> , 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," <i>Computer Networks</i> , 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	FreeSWAN Project, <i>Linux FreeSWAN Compatibility Guide</i> (March 4, 1999). (FreeSWAN Compatibility Guide, FreeSWAN)	

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	14	of	52	Attorney Docket Number	11798.0005

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, <i>Distributing Kerberos KDC and Realm Information with DNS</i> <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). (Bhattacharya 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. <i>Check Point FireWall-1 Administration Guide</i> , 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, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , 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," <i>Mobile Computing and Communications Review</i> , 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	<i>Onion Routing</i> , "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 <i>Gauntlet Firewall For Unix User's Guide Version 5.0</i> (1999). (Gauntlet User's Guide - Unix, Firewall Products)	
	D131	Network Associates <i>Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0</i> (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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO			Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			<i>Control Number</i>	95/001,792	
			<i>Filing Date</i>	December 25, 2011	
			<i>First Named Inventor</i>	Victor Larson	
			<i>Art Unit</i>	3992	
			<i>Examiner Name</i>	Deandra M. Hughes	
Sheet	15	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>Gauntlet Firewall For Unix Getting Started Guide Version 5.0</i> (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates <i>Release Notes Gauntlet Firewall for Unix 5.0</i> (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates <i>Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0</i> (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. <i>Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1</i> (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne <i>Dynamic Virtual Private Networks</i> (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred <i>Dynamic Virtual Private Networks (DVPN)</i> (December 21, 1999) (Kindred DVPN, DVPN)	
	D140	Dan Sterne <i>et al. TIS Dynamic Security Perimeter Research Project Demonstration</i> (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred <i>Dynamic Virtual Private Networks Capability Description</i> (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 <i>Security Quickstart Task Update</i> (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 <i>Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan</i> (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.msp (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, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.msp (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, <i>available at</i> 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) <i>available at</i> 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	16	of	52	Attorney Docket Number	11798.0005

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), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) <i>available in</i> PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) <i>available in</i> PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) <i>available in</i> PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) <i>available in</i> PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) <i>available in</i> PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, <i>Essential Winlnet</i> 313-423 (Addison Wesley Longman 1998) (Essential Winlnet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) <i>available at</i> 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/technet/archive/winntas/proddocs/inetconctservice/bcgstart.msp (Internet Connection Services I)	
	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.msp (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, <i>available at</i> http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.msp (IE5 Corporate Development)	
	D165	Mark Minasi, <i>Mastering Windows NT Server 4</i> 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	<i>Hands On, Self-Paced Training for Supporting Version 4.0</i> 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), <i>available at</i> http://www.microsoft.com/technet/archive/winntas/maintain/feasability/pptpwp3.msp (MS PPTP)	
	D168	Kenneth Gregg, <i>et al.</i> , <i>Microsoft Windows NT Server Administrator's Bible</i> 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), <i>available at</i> 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	17	of	52	Attorney Docket Number	11798.0005

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, <i>NT Network Plumbing: Routers, Proxies, and Web Services</i> 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/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	
	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, <i>F-Secure NameSurfer</i> (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, <i>F-Secure VPN Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	D177	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, <i>F-Secure SSH2.0 for Windows NT and 95</i> (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, <i>F-Secure VPN+ Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, <i>F-Secure VPN+ 4.1</i> (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, <i>F-Secure SSH</i> (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	D185	F-Secure, <i>F-Secure VPN+</i> (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, <i>F-Secure Management Tools, Administrator's Guide</i> (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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	18	of	52	Attorney Docket Number	11798.0005

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, <i>F-Secure Desktop, User's Guide</i> (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., <i>VPN Policy Manager</i> (January 2000) (VPN Policy Manager)	
	D189	F-Secure, <i>F-Secure VPN+ for Windows NT 4.0</i> (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., <i>SafeNet/Security Center Technical Reference Addendum</i> (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., <i>System Description for VPN Policy Manager and SafeNet/SoftPK</i> (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., <i>About SafeNet / VPN Policy Manager</i> (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., <i>Gauntlet Internet Firewall, Firewall Product Functional Summary</i> July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., <i>Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0</i> (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, <i>Windows NT Terminal Server and Citrix Metaframe</i> (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, <i>Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame</i> (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., <i>Securing L2TP using IPSEC</i> (February 2, 1999)	
	D198	156. <i>Finding Your Way Through the VPN Maze</i> (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, <i>The Business Case for Secure VPNs</i> (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., <i>WatchGuard LiveSecurity for MSS Powerpoint</i> (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., <i>MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes</i> (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., <i>MSS Firewall Specifications</i> (1999)	
	D204	WatchGuard Technologies, Inc., <i>Request for Information, Security Services</i> (2000)	
	D205	WatchGuard Technologies, Inc., <i>Protecting the Internet Distributed Enterprise, White Paper</i> (February 2000)	
	D206	Air Force Research Laboratory, <i>Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)</i> (January 29, 1998)	
	D207	Technologies, Inc., <i>WatchGuard Firebox System Powerpoint</i> (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA <i>Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0</i> (September 21, 1998)	
	D209	BBN Information Assurance Contract, <i>TIS Labs Monthly Status Report</i> (March 16-April 30, 1998)	
	D210	DARPA, <i>Dynamic Virtual Private Network (VPN) Powerpoint</i>	
	D211	GTE Internetworking, <i>Contractor's Program Progress Report</i> (March 16-April 30, 1998)	
	D212	Darrell Kindred, <i>Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization</i> (January 30, 2001)	
	D213	<i>Virtual Private Networking Countermeasure Characterization</i> (March 30, 2000)	
	D214	<i>Virtual Private Network Demonstration</i> (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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	19	of	52	Attorney Docket Number	11798.0005

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, <i>Dynamic Virtual Private Networks (VPNs) and Integrated Security Management</i> (2000)	
	D216	Information Assurance/NAI Labs, <i>Create/Add DVPN Enclave</i> (2000)	
	D217	NAI Labs, <i>IFE 3.1 Integration Demo</i> (2000)	
	D218	Information Assurance, <i>Science Fair Agenda</i> (2000)	
	D219	Darrell Kindred et al., <i>Proposed Threads for IFE 3.1</i> (January 13, 2000)	
	D220	<i>IFE 3.1 Technology Dependencies</i> (2000)	
	D221	<i>IFE 3.1 Topology</i> (February 9, 2000)	
	D222	Information Assurance, <i>Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development</i> January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation</i> (2000)	
	D224	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.2</i> (2000)	
	D225	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)	
	D226	T. Braun et al., <i>Virtual Private Network Architecture</i> , Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - <i>PGP Total Network Security Suite, Dynamic Virtual Private Networks</i> (1999)	
	D228	Microsoft Corporation, <i>Microsoft Proxy Server 2.0</i> (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., <i>A Guide To Microsoft Proxy Server 2.0</i> (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, <i>Setting Server Parameters</i> (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, <i>Microsoft Proxy Server 2</i> (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., <i>MCSE Proxy Server 2 Study Guide</i> (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenhardt, <i>IIS 4 and Proxy Server 2</i> (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, <i>MCSE Test Success: Proxy Server 2</i> (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, <i>The Windows NT and Windows 2000 Answer Book</i> (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (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	<i>AutoSOCKS v2. 1</i> , Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, <i>Use of DNS to Distribute Keys</i> , 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	20	of	52	<i>Attorney Docket Number</i>	11798.0005

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; <i>Extended VPN Uses The Internet to Create Virtual Private Networks</i> , 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 Kosior, "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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	21	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	22	of	52	<i>Attorney Docket Number</i>	11798.0005

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. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)	
	D292	DPCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages. 3 0	
	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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	23	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidation Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidation 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	24	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	25	of	52	Attorney Docket Number	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	26	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	27	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	28	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO			Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			<i>Control Number</i>	95/001,792	
			<i>Filing Date</i>	December 25, 2011	
			<i>First Named Inventor</i>	Victor Larson	
			<i>Art Unit</i>	3992	
			<i>Examiner Name</i>	Deandra M. Hughes	
Sheet	29	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	30	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>VirnetX v. Microsoft</i> .	
	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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	31	of	52	Attorney Docket Number	11798.0005

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 Accessible 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/rfc/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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	32	of	52	Attorney Docket Number	11798.0005

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://www.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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	33	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	34	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	35	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	36	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	37	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	38	of	52	<i>Attorney Docket Number</i>	11798.0005

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, Gauntlet System and Gauntlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gauntlet System and Gauntlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gauntlet 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	39	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Astra Technologies Ltd, NEC Corporation, NEC Corporation of America and Astra USA, Inc.</i> , 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	40	of	52	Attorney Docket Number	11798.0005

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 <i>VirnetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.</i> , 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, (November 1998) 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	41	of	52	Attorney Docket Number	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	42	of	52	Attorney Docket Number	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	43	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	44	of	52	Attorney Docket Number	11798.0005

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 <i>VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Astra Technologies Ltd, NEC Corporation, NEC Corporation of America and Astra USA, Inc.</i> , 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

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	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	45	of	52	Attorney Docket Number	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	46	of	52	<i>Attorney Docket Number</i>	11798.0005

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 7,921,211 relative 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	47	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>Inter Partes</i> Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate <i>Inter Partes</i> Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate <i>Inter Partes</i> 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, <i>VirnetX, Inc. v. Microsoft Corp.</i> , 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	48	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	49	of	52	<i>Attorney Docket Number</i>	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	50	of	52	Attorney Docket Number	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	51	of	52	Attorney Docket Number	11798.0005

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Receipt date: 09/20/2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	52	of	52	<i>Attorney Docket Number</i>	11798.0005

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	/Deandra Hughes/ (04/09/2013)	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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972
22852	7590	03/12/2013	EXAMINER HUGHES, DEANDRA M	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			03/12/2013	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
HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Date:

MAILED

MAR 12 2013

CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792
PATENT NO. : 7188180
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

FINNEGAN, HENDERSON, FARABOW,
GARRET & DUNNER LLP
901 New York Avenue, N.W.
Washington, D.C. 20001-4413

(For Patent Owner)

MAILED

MAR 12 2013

CENTRAL REEXAMINATION UNIT

David McCombs
Haynes and Boone, LLP
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

(For Third Party Requester)

Inter Partes Reexamination Proceeding
Control No.: 95/001,792
Filed: October 25, 2011
For: U.S. Patent No. 7,188,180

: **DECISION**
: **DISMISSING PETITION**
: **TO SHORTEN RESPONSE**
: **PERIODS AND**
: **ACCELERATE PROCEEDINGS**

This is a decision on third party requester's "Revised Petition Under 37 CFR § 1.182 To Shorten Response Periods and Accelerate Proceedings" ("petition under 1.182"), filed on January 11, 2013 and on "Patent Owner's Petition In Opposition To Third-Party Requester Cisco Systems, Inc.'s Revised Petition To Shorten Response Periods and Accelerate Proceedings" (the opposition"), filed on January 17, 2013.

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 proceedings.

BACKGROUND

1. On March 6, 2007, U.S. Patent No. 7,188,180 ("the '180 patent") issued to Larson et al. with 41 claims.

2. On August 11, 2010, VirnetX Inc. (“patent owner”) asserted the ‘180 patent and U.S. Patent Nos. 6,502,135, 7,418,504, 6,839,759 and 7,490,151 in the Eastern District of Texas (*VirnetX Inc. v. Cisco Sys., Inc., et al.*, No. 6:10-cv-00417). Patent owner additionally asserted U.S. Patent No. 7,921,211 in an Amended Complaint filed on April 5, 2011.
3. On October 25, 2011, a request for *inter partes* reexamination of the ‘180 patent was filed by a third party requester, which request was assigned control no. 95/001,792 (“the ‘1792 proceeding”). The request identified Cisco Systems, Inc. (“Cisco”) as the real party in interest. On September 6, 2012, the Office issued an order granting the request for *inter partes* reexamination in the ‘1792 proceeding.
4. On January 11, 2013, Cisco filed the instant petition paper entitled “Revised Petition Under 37 CFR § 1.182 To Shorten Response Periods and Accelerate Proceedings” (“the petition under 37 CFR 1.182”) in the merged proceeding.
5. Also, on January 11, 2013, Cisco filed petition papers entitled “Revised Petition Under 37 CFR § 1.182 To Shorten Response Periods and Accelerate Proceedings” in Reexamination Control Nos. 95/001,682; 95/001,697; 95/001,746; 95/001,851; and 95/001,856.
6. On January 17, 2013, patent owner filed “Patent Owner’s Petition In Opposition To Third-Party Requester Cisco Systems, Inc.’s Revised Petition To Shorten Response Periods and Accelerate Proceedings” (“the opposition”) in the merged proceeding.

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.

Cisco's Petition under 37 CFR 1.182 and Patent Owner's Opposition

In the petition under 37 CFR 1.182, Cisco ("petitioner") requests that "the Patent Office accelerate and bring to a close the various long-pending reexaminations, including setting shortened statutory periods for future Patent Owner responses."¹ Specifically, petitioner requests that "the schedules and handling of the following reexaminations² be accelerated, including that future Office Actions set a one-month (or 30 days, whichever is longer) period for response by the Patent Owner."³

In support of its request, petitioner cites to MPEP § 2662(L) which provides as follows:

(L) Litigation.

Where the reexamination results from a court order or litigation is stayed for purposes of reexamination, the shortened statutory period will generally be set at one month or thirty days, whichever is longer. In addition, if (1) there is litigation concurrent with an *inter partes* reexamination proceeding and (2) the reexamination proceeding has been pending for more than one year, the Director of the Office of Patent Legal Administration (OPLA), Director of the Central Reexamination Unit (CRU), Director of the Technology Center (TC) in which the reexamination is being conducted, or a Senior Legal Advisor of the OPLA, may approve Office actions in such reexamination proceeding setting a one-month or thirty days, whichever is longer, shortened statutory period for response rather than the two months usually set in reexamination proceedings. A statement at the end of the Office action – "One month or thirty days, whichever is longer, shortened statutory period approved," followed by the signature of one of these officials, will designate such approval. See MPEP § 2686.04.<

Petitioner asserts that because "[a]ll of the patents in reexamination are involved in co-pending litigations," and "[s]ince all of the reexamination proceedings are past or near their filing anniversaries, Cisco asks that a one-month (or 30 day) deadline be set for the Patent Owner's response to any Office Action issuing after a proceeding has been pending for more than a year."⁴ Petitioner also asserts that "[c]onsistent with the need for special dispatch, Cisco also believes that the Patent Office should enforce the shortened period for response by denying any further requests by the Patent Owner to delay the proceeding by extending its deadlines."⁵

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 Cisco."⁶ Patent owner further asserts that "accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would also

¹ Petition under 37 CFR 1.182 at page 2.

² The listed reexamination proceedings are the instant proceeding and Reexamination Control Nos. 95/001,682; 95/001,697; 95/001,746; 95/001,851; and 95/001,856.

³ Petition under 37 CFR 1.182 at page 3.

⁴ *Id.* at page 3-4.

⁵ *Id.* at page 4.

⁶ Opposition at page 4.

substantially prejudice Patent Owner”⁷ and would “unreasonably burden Patent Owner and its counsel.”⁸

Discussion

Petitioner requests that the Office accelerate the instant merged proceeding by (1) setting a one-month (or 30 day) deadline for future patent owner responses and (2) denying any further requests by patent owner for extensions of time. Petitioner’s request relates to matters that are discretionary on the part of the Office and which are decided by the Office on a case-by-case basis. For example, MPEP § 2662(L), relied upon by petitioner, makes clear that setting a shortened statutory period for patent owner responses is a matter of Office discretion.⁹ Such determination is made by balancing the desire to provide the patent owner with a fair opportunity to respond against the requirement of the statute that the proceedings be conducted with special dispatch. In this instance, patent owner has asserted that accelerating the proceedings would “unreasonably burden Patent Owner and its counsel.”¹⁰ Further, as noted by patent owner, “these reexaminations are already being appropriately conducted by the Office with the ‘special dispatch’ sought by Cisco.”¹¹

Additionally, MPEP § 2667(II)(B)(4), makes clear that granting a patent owner’s request for extension of time is also a matter of Office discretion.¹² Neither 35 U.S.C. § 314 (b)(2) nor the regulations provide any right for the third party requester to file an opposition or comment on a patent owner’s request for an extension of time under 37 CFR 1.956.¹³ This is an issue that goes to timeliness, rather than to the merits. While enactment of the *inter partes* reexamination statute was for the purpose of expanding a third party requester’s participation in the *merits* of the proceeding, there is no indication whatsoever in the legislative history of the *inter partes* reexamination statute that the requester was granted any right to challenge the granting of an extension of time in an *inter partes* reexamination proceeding. The lack of such a right was not raised in the enactment of the *inter partes* reexamination statute (or in any of the precursor bills),

⁷ *Id.* at page 5.

⁸ *Id.* at pages 5-6 (noting that patent owner “must also respond to filings from Apple in a large number of other reexaminations.”)

⁹ MPEP § 2662(L) specifically states “the Director of the Office of Patent Legal Administration (OPLA), Director of the Central Reexamination Unit (CRU), Director of the Technology Center (TC) in which the reexamination is being conducted, or a Senior Legal Advisor of the OPLA, may approve Office actions in such reexamination proceeding setting a one-month or thirty days, whichever is longer, shortened statutory period for response rather than the two months usually set in reexamination proceedings” (emphasis added).

¹⁰ *Id.* at pages 5-6 (noting that “Along with these proceedings, Patent Owner is concurrently involved in five additional reexaminations naming Apple as the real party in interest, which are also demanding significant attention from Patent Owner.”)

¹¹ Opposition at page 4.

¹² MPEP § 2667(II)(B)(4) states that “any petition requesting that an extension of time be denied will be returned, since a requester does not have a statutory right to challenge this discretionary procedural process in the reexamination proceeding; whether or not the time is extended clearly does not go to the merits of the reexamination proceeding.”

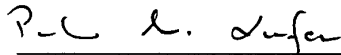
¹³ See *Streamlined Patent Reexamination Proceedings; Notice of Public Meeting*, 76 Fed. Reg. 22854, 22858 (April 25, 2011) (stating that a patent owner’s request for extension of time to respond to an Office action in *inter partes* reexam is not opposable).

and there is no evidence to indicate that enacting such a right was ever contemplated by Congress.

To the extent petitioner is requesting that the Office bind itself at the present time to a particular course of action in the future, the Office declines. Any future decisions by the Office to exercise its discretion with respect to this matter will be decided on a case-by-case basis, balancing the equities noted above. Accordingly, for at least the aforementioned reasons, **the petition under 1.182 is dismissed.**

CONCLUSION

1. Petitioner's January 11, 2013 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



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.
-----------------	-------------	----------------------	---------------------	------------------

95/001,792	10/25/2011	7,188,180	43614.100	1972
------------	------------	-----------	-----------	------

22852 7590 02/27/2013
 FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
 LLP
 901 NEW YORK AVENUE, NW
 WASHINGTON, DC 20001-4413

EXAMINER

HUGHES, DEANDRA M

ART UNIT	PAPER NUMBER
----------	--------------

3992

MAIL DATE	DELIVERY MODE
-----------	---------------

02/27/2013

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 <i>Inter Partes</i> Reexamination	Control No.	Patent Under Reexamination	
	95/001,792	7,188,180	
	Examiner	Art Unit	
	Deandra M. Hughes	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Haynes and Boone, LLP
IP Section
2323 Victory Avenue Suite 700
Dallas, TX 75219

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.

ACTION CLOSING PROSECUTION (37 CFR 1.949)	Control No.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	Deandra M. Hughes	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 19 December, 2012

Third Party(ies) on 16 January, 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 1,4,6-17,20,22-33,35 and 37-41 are subject to reexamination.
- 1b. Claims _____ are not subject to reexamination.
2. Claims _____ have been canceled.
3. Claims 1,4,6-17,20,22-33,35 and 37-41 are confirmed. [Unamended patent claims]
4. Claims _____ are patentable. [Amended or new claims]
5. Claims _____ 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 _____

INTER PARTES REEXAMINATION ACTION CLOSING PROSEUTION

1. This is an action closing prosecution (“ACP”) in the *inter partes* reexamination of **claims 1, 4, 6-17, 20, 22-33, 35 and 37-41** of USP 7,188,180. (“**180 patent**”)

- Patent Owner’s remarks (hereafter “remarks”) filed Dec. 19, 2012 have been entered.
- Third Party Requester’s comments (hereafter “comments”) filed Jan. 16, 2012 have entered.

Evidence Cited in this Action

2. The evidence is cited in this action:

- (A) Kiuchi et al. “*The Development of a Secure, Closed HTTP-based Network on the Internet*”, 1996. (“**Kiuchi**”)
- (B) Martin, David M. “*A Framework for Local Anonymity in the Internet*”, February 21, 1998. (“**Martin**”)
- (C) RFC973: Information Sciences Institute, “Transmission Control Protocol”. DARPA Internet Program Protocol. Sept. 1981. (“**RFC973**”)
- (D) Declaration of Dr. Angelos D. Keromytis, Ph.D. executed Dec. 16, 2012. (“**Keromytis Declaration**”)
- (E) Declaration of Dr. Robert Dunham Short III, Ph.D. executed Dec. 18, 2012. (“**Short Declaration**”)

Response to PO's Remarks and 3PR's Comments

I. *Summary of Kiuchi*

Kiuchi discloses "C-HTTP" which provides secure HTTP communications within a closed group of institutions on the internet, where each member is protected by its own firewall. (*Abstract*) **Kiuchi** discloses that these C-HTTP-based communications are made possible by three components: (1) a client-side proxy, (2) a server-side proxy, and (3) a C-HTTP name server. (*Id.*) The client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol, while communications between a user agent and client-side proxy or an origin server and server-side proxy are performed using HTTP/1.0. (*Id.*) In a C-HTTP-based network, instead of DNS, a C-HTTP-based secure, encrypted name, and certification service is used. (*Id.*)

II. *Claim 1: "sending an access request message to the secure computer network address using a virtual private network communication link."*

As to this claim limitation, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi's** disclosed "request for connection to the server-side proxy" of *Appendix 3(c)* reads on the claimed "access request message" and the disclosed "C-HTTP connection between a client-side proxy and a server-side proxy" reads on the claimed "virtual private network communication link". (*Claim Charts, Exhibit E-2, pg. 13-16*)

PO argues **Kiuchi's** claimed "request for connection" of *Appendix 3(c)* is sent before any C-HTTP connection is established, and accordingly **Kiuchi** fails to disclose "sending an access request message...using a virtual private communication link" because the "access request message" (i.e., request for connection) cannot use a

Art Unit: 3992

virtual private communication link (i.e., the C-HTTP connection) that has not yet been established. (*Remarks, pg. 6; emphasis added*)

PO also provides the **Keromytis Declaration**, which makes the following statement as to **Kiuchi** (§23):

23. A person of ordinary skill in the art at the time of the invention would also have understood that the mere two steps of (1) contacting a name server to obtain a server-side proxy's public key, and then (2) using that public key to encrypt a request for connection, do not thereby create a "virtual private network communication link." This is because, in this situation, no "link" exists at all between the client-side and server-side proxies at the time the "request for connection" is sent. Rather, there is only a one-way communication sent as part of *setting up* the C-HTTP connection. (*Kiuchi 64-65.*)

3PR responds that when the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, the client-side proxy sends a request for connection to the server-side proxy's public key. (*Comments, pg. 2 lines 3-6 citing Kiuchi at p.65*)

Upon examination of **Kiuchi**, it is found the claim term 'private' modifies the claim term 'network' and as such, **Kiuchi** must teach the 'privacy' of the 'network' and not just the privacy of the 'communication link' to anticipate the claims.

Second, it is found that **Kiuchi** discusses a 'virtual network' only once, which is reproduced below.

5. Concluding remarks

Although C-HTTP is primarily developed for use in the medical field, it can be used in other areas. Using C-HTTP, a closed HTTP-based virtual network can be constructed for closed groups, for example, the headquarters and branches of a given corporation. This kind of usage may not fit with the spirit of the Internet, but if resources which might otherwise be invested in private circuits are channeled into the Internet, it will contribute to its further development.

Third, it is found that this disclosure by **Kiuchi** that "[u]sing C-HTTP, a closed HTTP-based virtual network can be constructed for closed groups" applies to the C-HTTP that is established *in response* to a "request for connection to the server-side proxy" of *Appendix 3(c)* because the request for connection occurs *before* the C-HTTP (i.e. the virtual private network communication link) is established.

As such, it is agreed that **Kiuchi** does not disclose "*sending an access request message...using a virtual private communication link*" because **Kiuchi** discloses that the '*access request message*' (i.e. the request for connection) occurs before a '*virtual private communication link*' (i.e. the C-HTTP) has been established and therefore cannot use the said link. (*Appendix 3(c)*) Therefore, for at least this reason, the anticipation rejection of **claims 1, 4, and 6-16** under **Kiuchi** is withdrawn.

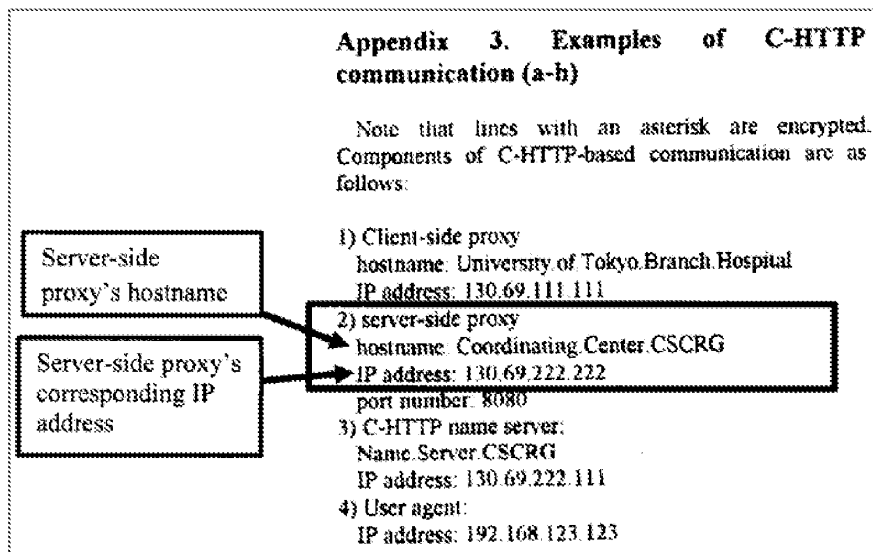
III. *Claim 1: "the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name"*

As to this claim limitation, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi's** disclosed `Coordinating.Center.CSCRG` reads on the claimed "*secure domain name*" and the disclosed secure server-side proxy IP address reads on the claimed "*secure computer network address*". (*Claim Charts, Exhibit E-2, pgs. 9-10*)

PO argues **Kiuchi's** URL (i.e. the claimed 'secure domain name') does not correspond to the server-side proxy, but rather the resource itself located on an origin server. (*Remarks, pg. 8, lines 3-5*) The **Keromytis Declaration** does not address this claim limitation.

3PR responds that PO ignores the example in *Appendix 3(a) and 3(b)* of **Kiuchi**, where **Kiuchi** teaches an embodiment in which the IP address returned by the name server is the IP address that directly corresponds to the hostname contained in the query message. (*Comments, pg. 4, 1st ¶*)

Upon examination of **Kiuchi**, it is found that **Kiuchi's Appendix 3:Examples of C-HTTP Communication (a-h)**, which is reproduced below with 3PR's annotations, discloses that the claimed "secure domain name" (i.e., `Coordinating.Center.CSCRG`) corresponds to the claimed "secure computer network address" (i.e., IP address: `130.69.222.222`). As such, PO's argument is not persuasive.



However, for the reason that **Kiuchi** does not disclose "*sending an access request message...using a virtual private communication link*", as discussed above, the anticipation rejection of **claim 1** under **Kiuchi** is withdrawn.

Art Unit: 3992

IV. Claims 17 and 33

PO incorporates by reference the arguments traversing the rejection of **claim 1** over **Kiuchi**. As such, the response to these arguments, as set forth above, is incorporated here. Therefore, for at least the reason incorporated here, the anticipation rejection of **claims 17, 20, 22-33, 35, and 37-41** under **Kiuchi** is withdrawn.

V. Claims 6, 22, and 37

As to the claim limitation "*the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network*", the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that, *inter alia*, the value in the allegedly inherent 'type of service field' in the TCP/IP session disclosed by **Kiuchi** reads on the claimed 'data value'. (*Claim Charts, Exhibit E-2, pgs. 21-22 citing RFC 793 to support inherency*)

PO argues **Kiuchi** does not specifically or inherently disclose this limitation because the evidence (*i.e.*, *RFC 793 at p. 12*) does not support the conclusion that **Kiuchi's** C-HTTP system would necessarily insert into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network. (*Remarks, pg. 9, last ¶*)

PO also provides the **Keromytis Declaration**, which makes the following statement as to **Kiuchi** (*¶27*):

Art Unit: 3992

27. *Kiuchi* simply does not describe any nexus between RFC 793's "type of service" fields and the alleged virtual private network (i.e., the C-HTTP connection) or a predetermined level of service associated with a C-HTTP connection. Thus, a person of ordinary skill would not have understood *Kiuchi*'s C-HTTP connection to be "based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network." Accordingly, a person of ordinary skill would not have understood *Kiuchi* to show, either expressly or inherently, that "the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network," as recited in claims 6, 22, and 37.

3PR responds that **Kiuchi** discloses this limitation because **Kiuchi** discloses inserting version information (e.g., C-HTTP Version = 'C-Http/0.7') in the request and into the response. (*Comments*, pg. 6, last ¶, citing *Kiuchi* at 70, 71) 3PR argues the C-HTTP version value inserted into the request and the response defines the "version of C-HTTP name service protocol" being used. (*Comments*, pg. 6, last ¶, citing *Kiuchi* at 72) Further, 3PR states the version of the name service protocol is a data value representing a predetermined level of service. (*Comments*, pg. 6, last ¶) Accordingly, 3PR argues that **Kiuchi** discloses "the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network" because **Kiuchi** inserts version information defining the name service into each request and response, (*Comments*, pg. 6, 1st ¶)

Upon examination of **Kiuchi**, it is found that 3PR's argument as to 'inserting version information' was not presented in the request and claim charts (*see Exhibit E-2*, pgs. 21-22, 35, and 37). As such, PO has not yet had an opportunity to address this materially different and newly presented version of the anticipation rejection of **claims 6, 22, and 37** under **Kiuchi**. Nonetheless, 3PR's argument is not persuasive because it is

Art Unit: 3992

found that **Kiuchi's** C-HTTP Version = 'C-Http/0.7' is not inserted into a data packet, as claimed, but rather the C-HTTP version is transmitted as request-line or a version-line, respectively. (*Kiuchi pg. 70 at §2.1 and pg. 71 at §2.1*) Therefore, for this additional reason, the anticipation rejection of **claims 6, 22 and 37** under **Kiuchi** is withdrawn.

VI. Claims 8, 24, and 39

As to the claim limitation "*the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values*", the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that, *inter alia*, **Kiuchi's** disclosed nonce values reads on the claimed "*value in each data packet*". (*Claim Charts, Exhibit E-2, pgs. 22-25*)

PO argues **Kiuchi** does not anticipate these claims because they do not specifically or inherently disclose this limitation because **Kiuchi** does not disclose (1) comparing the nonce header field to a 'moving window of values' or (2) the nonce values are inserted into each data packet. (*Remarks, pg. 10*)

As to PO's first argument, PO argues **Kiuchi** does not disclose this claim limitation because **Kiuchi** at *pg. 74*, which discusses incrementing the Request-Nonce value, teaches that different types of requests might contain different nonce values. (*Remarks, pg. 10, 2nd ¶*) PO argues that this disclosure does not, however, teach that **Kiuchi's** nonce values are compared to a "*moving window of valid values*", as claimed. (*Id.*) Further, PO argues, there are many ways the values of **Kiuchi's** nonce header field could be checked without comparing them to a moving window of valid values. (*Id.*) PO

Art Unit: 3992

provides the **Keromytis Declaration** as opinion evidence to support PO's arguments.

(¶¶29-30)

3PR responds that PO's arguments contradict the specification of the '**180 patent**, which allegedly defines a "moving window of values" as "1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence." (*Comments, pg. 8 last ¶ citing '180 patent, col.11:59-61*)

Upon examination of the '**180 patent**, it is found that *col.11:59-61* defines a 'window sequence number' but does not define a 'moving window of values', as argued by PO. This portion of the '**180 patent** is reproduced below:

In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information 55 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.

As such, for the reason that 3PR's argument is premised on an erroneous claim construction, i.e., that the claim limitation 'moving window of values' is defined as the disclosed 'window sequence number', this argument is not persuasive.

Further, assuming *arguendo*, that claim construction of 'moving window of values' is as 3PR argues, then this argument is not persuasive because it is found that the patterns 3PR allege are 'incremented' are merely different because '853f...8540...8541' and 'c99...c9a..c9b' do not suggest 'incrementation' because the differences between the nonce values are variable. The chart 3PR produced to support the 'incrementation' argument is reproduced below. (*Comments, pg. 8*)

Art Unit: 3992

Request-Nonce	Response-Nonce
8abd853f	ef23dc99
8abd8540	ef23dc9a
8abd8541	ef23dc9b

As to PO's second argument, PO argues **Kiuchi** does not disclose that the nonce value is inserted into each data packet because **Kiuchi** discloses that the C-HTTP requests and responses, and not the data packets, contain the nonce values. (*Remarks, pg. 10, last ¶*) PO also provides the **Keromytis Declaration** as opinion evidence to support PO's arguments. (*¶30*)

3PR responds that PO is importing limitations from the specification into the claims and that the specification of the '**180 patent** mentions many types of 'data packets' and does not limit them to the 'IP packet' or the 'ACK packet'. (*Comments, pg. 9, 2nd ¶*)

Upon examination of **Kiuchi**, it is found that **Kiuchi**'s request and responses, which include the nonce values, read on the broadest reasonable interpretation of 'data packet' because these data, including the nonce value, are included in a packet (i.e. a bundle). As such, PO's second argument is not persuasive.

Nonetheless, for the reason that it is agreed that **Kiuchi** does not disclose the claimed "moving window of values", the anticipation rejection of **claims 8, 24, and 39** under **Kiuchi** is withdrawn.

Art Unit: 3992

VII. Claims 9, 25, and 40

As to the claim limitation "*the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields*", the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi**'s disclosed connection ID field reads on the claimed "*discriminator field*". (*Claim Charts, Exhibit E-2, pgs. 22-25*)

PO argues **Kiuchi** does not specifically or inherently disclose this limitation because **Kiuchi**'s disclosed 'connection ID' is not inserted into a header of each data packet and **Kiuchi**'s virtual private network is not disclosed as *based on a comparison* of the disclosed 'connection ID'. (*Remarks, pg. 11*)

As to PO's first argument, PO argues **Kiuchi**'s 'connection ID' (i.e. the claimed 'discriminator field'), constitutes a portion of a resource name and is not "*in a header of each data packet*" as claimed.

3PR responds that PO is importing limitations from the specification into the claims and that the specification of the '**180 patent** mentions many types of 'data packets' and does not limit them to the 'IP packet' or the 'ACK packet'. (*Comments, pg. 10, 1st ¶*)

Upon examination of **Kiuchi**, it is found that the disclosed general-header contains the 'connection ID'. (*pg. 71, §1.3 item 7*) As such, PO's argument that **Kiuchi**'s 'connection ID' (i.e., the claimed 'discriminator field') is not "*in a header of each data*

Art Unit: 3992

packet", as claimed, is not persuasive because it is found that **Kiuchi**'s 'connection ID' is disclosed as part of the general header.

As to PO's second argument, PO argues that virtual private network is not disclosed as *based on a comparison* of the disclosed 'connection ID' (i.e., the claimed 'discriminator field') because **Kiuchi**'s C-HTTP, if anything, is based on a timer, not on a 'connection ID'. PO also provides the opinion evidence of the **Keromytis Declaration** to support his argument. (§33)

3PR responds that **Kiuchi** discloses this limitation because **Kiuchi** discloses that the 'connection ID' is compared against a table of current connections, and if the 'connection ID' is not found, then the connection is disconnected. (*Comments, pg. 10, 2nd ¶, citing Kiuchi at 65*)

Upon examination of **Kiuchi**, it is found the 'connection ID' is stripped from the original resource name and then the original name is forwarded to the server. (*Kiuchi at 65, col.1, 1st ¶*) It is also found that when the 'connection ID' is not found in the current connection table in the client-side proxy, the current connection is disconnected. (*Id.*) As such, PO's argument that the 'connection ID' is not compared to a table of valid discriminator fields is not persuasive because the 'connection ID' (i.e., the claimed '*discriminator field*') is disclosed as being compared to a table of current connections (i.e., the claimed '*table of valid discriminator fields*'). However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1, 17, and 33**, the anticipation rejection of **claims 9, 25, and 40** under **Kiuchi** is withdrawn.

Art Unit: 3992

VIII. Claims 12 and 28

As to this claim limitation, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues that **Kiuchi**'s requested connection information, including a connection ID and a second symmetric data exchange key, are provided by the server-side proxy. (*Claim Charts, Exhibit E-2, pg. 28*) As such, the rejection argues that the disclosed 'connection information' reads on the claimed '*requested information*' and the disclosed 'server-side proxy' reads on the claimed '*secure computer network address*'.

PO argues **Kiuchi** does not disclose that "*the access request message contains a request for information stored at the secure network address*" because **Kiuchi** discloses that the connection ID and symmetric data exchange key are not stored at the secure computer network address, as recited in the claims, but rather are newly generated after the server-side proxy receives information regarding the client-side proxy from the C-HTTP name server. (*Remarks, pg. 12*) PO also provides the **Keromytis Declaration** as opinion evidence to support this argument. (§35)

3PR responds the connection ID (e.g. the information requested) is generated then stored at the secure computer network address (e.g., the server-side proxy), because **Kiuchi** teaches the server-side proxy needs to delete the connection ID after the connection is closed (i.e., in order for it to be deleted, the connection ID must have first been stored). (*Comments, pg. 11, 2nd ¶*)

Upon examination of **Kiuchi**, it is found that the response from the server-side proxy indicating that the connection has been established includes the server-side-

Art Unit: 3992

proxy-IP address (130.69.222.222) and the server-side proxy name (i.e.

Coordinating.Center.CSCRG). (pg. 74, section f) As such, it is agreed that the disclosed 'connection information' reads on the claimed '*requested information*' and the disclosed 'server-side proxy' reads on the claimed '*secure computer network address*'.

However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1 and 17**, the anticipation rejection of **claims 12 and 28** under **Kiuchi** is withdrawn.

IX. Claims 13, 15, 29, and 31

As to these claims, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues, *inter alia*, that **Kiuchi**'s disclosed 'client-side proxy' reads on the claimed 'client computer'.

(*Claim Charts, Exhibit E-2, pg. 29*)

PO argues that the client-side proxy does not read on the claimed 'client computer' because **Kiuchi** clearly distinguishes between clients and client-side proxies. (*Remarks, pg. 12*) According to PO, **Kiuchi** describes 'user agents' as entities with a firewall, while explaining that the client-side proxy resides on the firewall of an institution. (*Remarks, pg. 12, 3rd ¶ citing Kiuchi at 64*)

PO also provides the **Keromytis Declaration** as opinion evidence stating that a person of ordinary skill at the time of the invention would have been readily capable of distinguishing, as **Kiuchi** does, between client computers within an institutional firewall (e.g. a nurse's or doctor's PC in a hospital) and a client computer residing on an institutional firewall (e.g. a client-side proxy). (*¶38*)

3PR responds that **Kiuchi** teaches a user agent that communicates with a client-side proxy. (*Comments, pg. 12, 3rd ¶*) According to 3PR, a user enters a hostname into the user agent (e.g., a nurse's PC in a hospital), which sends the hostname to the client-side proxy. (*Id.*) Accordingly, 3PR argues, the client-side proxy receives the hostname and the hostname was from the user. (*Id.*) Thus, 3PR concludes, **Kiuchi** discloses the method occurring at and being performed by the client computer. (*Id.*)

In response to PO's argument that **Kiuchi**'s 'user agent' and 'client-side proxy' do not read on the claimed 'user' and 'client computer', respectively, because **Kiuchi** describes 'user agents' as within a firewall, while explaining that the client-side proxy resides on the firewall of the institution, it is noted that the features upon which PO relies (i.e., 'within a firewall' or 'on the firewall') are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As such, PO's argument is not persuasive. However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1, 17, and 33**, the anticipation rejection of **claims 13, 15, 29, and 31** under **Kiuchi** is withdrawn.

X. Claims 16 and 32

As to **claims 16 and 32**, it is agreed that the rejection of these claims is improper for the reason that **claims 16 and 32** depend upon claims **claims 2 and 18**, respectively, for which no RLP was found. (*see Order at 10-11*) Accordingly, the rejection of **claims 16 and 32** is withdrawn.

Art Unit: 3992

XI. Claims 4, 10, 14, 20, 26, 30, and 35

PO incorporates by reference the arguments traversing the rejection of **claims 1, 17, and 33** over **Kiuchi**. As such, the response to these arguments, as set forth above, is incorporated here. Therefore, for at least the reason incorporated here, the anticipation rejection of **claims 4, 10, 14, 20, 26, 30, and 35** under **Kiuchi** is withdrawn.

XII. Claims 11, 27, and 41

As to these claims, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues, *inter alia*, that the claims are obvious over **Kiuchi** because adding an 's' to indicate a secure domain to conventional domain names such as .com, .net, .org, .edu, .mil, or .gov is a design choice within the knowledge and skill in the art. (*Claim Charts, Exhibit E-2, pgs. 51-52*)

First, PO argues that the request and claim charts fail to provide the requisite articulated reasoning to support the rejection. (*Remarks, pg. 13*)

3PR responds that rearranging letters is a mere design choice. (*Comments, pg. 13*)

Upon examination, it is found that the request and claim charts, as explained in the Petition Decision (mailed 9/26/2012, pg. 14) provide a reasonable rationale for modifying **Kiuchi** because one of ordinary skill in this art would know that the added letter 's' stands for 'security'. As such, PO's argument that the rejection does not set forth the requisite 'articulated reasoning' is not persuasive because the rationale for the design choice is that it is known in the art that 's' stands for 'security'.

Second, PO argues that **Kiuchi's** taught domain names does not disclose or suggest succinctly modifying a top-level domain name to denote security; rather, PO argues, **Kiuchi's** allegedly lengthy and unwieldy domain names suggests the exact opposite. (*Remarks, pg. 14, 2nd ¶*)

3PR responds that PO is attempting to import limitations from the specification in the claims because the claims recite nothing about 'denoting security'. (*Comments, pg. 13, 4th ¶*)

Upon examination, it is found that PO's argument is not persuasive. In response to PO's argument that there is no teaching, suggestion, or motivation in **Kiuchi** that makes obvious the claim limitation, the examiner recognizes that obviousness may be established by modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

In this case, **Kiuchi** discloses the 'user agent to client-side proxy' and the 'server-side proxy to origin server' are HTTP/1.0 connections. (pg. 64, §2.1) It is well-known that HTTP/1.0 connections use conventional top-level domain names such as .com, .net, .org, .edu, .mil, or .gov. Further, it is well-known to one of ordinary skill in the art that modifying a conventional domain name with an 's' denotes security. As such, **Kiuchi** as modified by knowledge generally available in the art, i.e. HTTP/1.0

Art Unit: 3992

connections use conventional top-level domain names such as .com, .net, .org, .edu, .mil, or .gov and that 's' denotes security, makes obvious the claim limitations. As such, PO's arguments are not persuasive. However, for the reason that it is agreed that **Kiuchi** does not anticipate base claims 1, 17, and 33, the rejection of claims 11, 27, and 41 as obvious over **Kiuchi** in view of **Martin** is withdrawn.

XIII. Claims 7, 23, and 38

As to these claims, the request and claim charts, which were adopted and incorporated by reference in the non-final rejection mailed Sept. 19, 2012, argues, *inter alia*, that although **Kiuchi** does not disclose this limitation, **Martin** teaches an IP hopping scheme because "[c]hoosing one of the source addresses 'at random' shows establishing the virtual private network communication link through pseudo randomly changing computer network addresses as recited by the claim." (*Claim Charts, Exhibit E-2, pgs. 48-50 citing Martin at pg. 9*)

PO argues that 3PR's tangential assertion that **Martin** describes choosing one of the source addresses at random, does not teach the claimed "*pseudo-randomly changing network addresses in packets, let alone a network address hopping regime that is used to pseudo-randomly change network addresses in packets.*" (*Remarks, pg. 15*)

3PR responds that "[r]andomly using different network addresses for each connection as taught by the combination of **Kiuchi** and **Martin** teaches that the source and destination network addresses in the packets transiting the virtual private network randomly change". (*Comments, pg. 15*)

Upon examination, it is found that **Martin** teaches the following (pg. 9):

4.4 Indirect Connection Addressing

Indirect addressing is straightforward but expensive. Let A_{IP} be the set of anonymous IP addresses in the lanon. $PORT = \{0, 1, \dots, 2^{16} - 1\}$ be the set of possible port numbers, and $A_{TCP} = A_{IP} \times PORT$ be the set of all possible TCP endpoint connection identifiers. Each such identifier is called an *anonymous TCP address*. A lanon client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random subject to lanon uniqueness and application-specific constraints.

Randomly choosing the source label hides the node's identity from external (and internal) observers. Later,

It is found that **Martin's** A_{TCP} , which is disclosed as the set of all possible TCP endpoint connection identifiers, reads on the claimed 'computer network addresses'. Further, **Martin** teaches a lanon client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random. As such, it is found that **Martin** teaches the claimed "*computer network address hopping regime*" because **Martin** teaches selecting its source address/port pair from A_{TCP} at random. Therefore, PO's arguments are not persuasive. However, for the reason that it is agreed that **Kiuchi** does not anticipate base **claims 1, 17, and 33**, the rejection of **claims 7, 23, and 38** as obvious over **Kiuchi** in view of **Martin** is withdrawn.

XIV. Secondary Considerations of Obviousness

"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 and therefore the examiner must determine whether there is a nexus between the merits of the claimed invention and the evidence of secondary considerations." MPEP §716.01(b)

1. Long Felt Need

As to the evidence of long felt need for the claim language pertaining to “receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link”, PO provides the **Short Declaration** (§§3-8).

The first example of long felt need provided by the **Short Declaration** (§§4-5) lacks the requisite nexus with the claim language because the evidence pertaining to the DARPA programs 'Information Assurance' and 'Dynamic Coalitions' identifies a general need for creating secure groups rapidly but does not identify the long felt need for “receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link”, as claimed. More importantly, the evidence lacks the requisite nexus because it does not discuss ‘secure domain name services’, ‘secure computer network address’, ‘access request messages’, or a ‘virtual private communication link’.

The second example regarding In-Q-Tel's willingness to enter into a relationship with SAIC (the original assignee of the application that led to the ‘**180 patent**’) for the development of the claimed technology lacks the requisite nexus with the said claim limitation because In-Q-Tel's willingness to enter into a relationship with SAIC may be due to other factors such as SAIC's size and reputation. (see **Short Declaration** §6)

Art Unit: 3992

More importantly, the evidence lacks the requisite nexus because it does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

As to the third example, the evidence of long felt need provided by the **Short Declaration** (§§7-11) lacks the requisite nexus with the claim limitation "*receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link*" because the evidence pertains to a general need for a secure VPN but does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

As such, the evidence of the long felt need provided by the **Short Declaration** is given very little weight because it lacks the requisite nexus with the claimed language.

2. Commercial Success

The **Short Declaration** provides evidence of SafeNet's portfolio license that includes the '**180 patent** and VirnetX's license agreement of \$200M as evidence of commercial success. (§12) This evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation "*receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link*" because the commercial success could be due to any number of market factors

Art Unit: 3992

including superior business acumen or marketing. More importantly, the evidence lacks the requisite nexus because it does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link' .

3. Skepticism

The **Short Declaration** provides evidence that the claimed invention was met with skepticism by others in the art before the inventor's work because Dr. Short argues that 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. (§§13-15) This evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation "*receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link*" because the evidence pertains to skepticism of an easy-to-set-up secure VPN connection but does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

4. Praise

The **Short Declaration** provides evidence that the claimed invention was met with praise by others because of the extensive licensing of the patented technology by Safenet, Microsoft, Aastra, Mitel, and NEC . (§§16) This evidence, however, is given very little weight because it lacks the requisite nexus with the claim limitation "*receiving*

Art Unit: 3992

from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private communication link" because the extensive licensing could have been motivated by a desire to avoid the costs of litigation and not by respect for the non-obviousness of the invention. More importantly, the evidence lacks the requisite nexus because it does not discuss 'secure domain name services', 'secure computer network address', 'access request messages', or a 'virtual private communication link'.

[The remainder of this page is intentionally left blank.]

Reasons for Confirming the Claims as Patentable

3. Independent **claims 1, 17, and 33** are confirmed as patentable over **Kiuchi**, alone or in combination, because **Kiuchi** does not disclose or make obvious “*sending an access request message to the secure computer network address using a virtual private network communication link*” in combination with the other limitations of the claims.

It is found that **Kiuchi** does not disclose or make obvious this claim limitation because the disclosed 'request for connection' of *Appendix 3(c)* (i.e., the claimed "access request message") is sent before the C-HTTP (i.e., the claimed "virtual private network communication link") and as such, the disclosed 'request for connection' does not use the C-HTTP (i.e. the claimed “virtual private network link”), as claimed, because no link exists at all between the disclosed client-side and server-side proxies at the time the ‘request for connection’ is sent. As such, the rejections over **Kiuchi** as set forth in the request and claim charts, are withdrawn and the claims are confirmed as patentable over **Kiuchi**. Further, **Claims 4, 6-16, 20, 22-32, 35, and 37-41** are confirmed as patentable for at least the reason that they are dependent upon confirmed based **claims 1, 17, and 33**.

[The remainder of this page is intentionally left blank.]

Conclusion

4. For the reasons set forth above, the rejections of **claims 1, 4, 6-17, 20, 22-33, 35, and 37-41**, as set forth in the request and claim charts, are withdrawn. As such, these claims are confirmed as patentable over the prior art of record.

5. **This is an ACTION CLOSING PROSECUTION (ACP)**; see MPEP § 2671.02.

6. 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.

7. 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.

8. 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).

9. Appeal cannot be taken from this action, since it is not a final Office action.

10. All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: Central Reexamination Unit

Art Unit: 3992

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

11. 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.

12. Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties 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).

Art Unit: 3992

13. 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 concurrent proceeding, involving this patent 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 throughout the course of this reexamination proceeding. See MPEP §2686 and 2686.04.

14. Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.


Signed:

/Deandra M Hughes/
Primary Examiner, Art Unit 3992

Conferees:

/Christina Y. Leung/
Primary Examiner, Art Unit 3992

/Daniel J Ryman/
Supervisory Patent Examiner, Art Unit 3992

Reexamination 	Application/Control No. 95001792	Applicant(s)/Patent Under Reexamination 7,188,180
	Certificate Date	Certificate Number

Requester Correspondence Address:	<input type="checkbox"/> Patent Owner	<input checked="" type="checkbox"/> Third Party
David L. McCombs HAYNES and BOONE LLP 2323 Victory Avenue, Suite 700 Dallas, TX 75219		

LITIGATION REVIEW <input checked="" type="checkbox"/>	DMH <small>(examiner initials)</small>	08/25/2012 <small>(date)</small>
<small>Case Name</small>		<small>Director Initials</small>
Virnetx v. Cisco et al. 6:10cv417 (OPEN)		
Virnetx v. Microsoft 6:10cv94 (CLOSED)		
VirnetX v. Microsoft 6:07cv0080		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

--	--



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972

22852 7590 01/24/2013
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

HUGHES, DEANDRA M

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:

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792

PATENT NO. : 7188180


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 Expunging/Returning Papers in Reexamination	Control No.: 95/001,792
<p>1. <input checked="" type="checkbox"/> THIS IS A DECISION EXPUNGING THE PAPER(S) FILED: <u>05 December 2012</u> by <u>requester</u> from the record of the reexamination proceeding(s). Since each expunged paper does not form part of the record, it is being expunged by marking it "closed" and "not public" in the Office's Image File Wrapper (IFW) system.</p> <p><input type="checkbox"/> THIS IS A DECISION RETURNING/DESTROYING THE PAPER(S) FILED _____ by _____.</p> <p>2. The papers being <input checked="" type="checkbox"/> expunged <input type="checkbox"/> returned <input type="checkbox"/> destroyed are: <u>Petition Under 37 CFR § 1.182 to Shorten Response Periods.</u></p> <p style="padding-left: 40px;">This decision will be made of record in the reexamination file(s).</p> <p>3. THE ABOVE-IDENTIFIED PAPERS LACK A RIGHT OF ENTRY BECAUSE:</p> <p>A. <input type="checkbox"/> Patent Owner may not file papers in the record prior to the order granting/denying reexamination (<i>ex parte</i>) or first action (<i>inter partes</i>). 37 CFR §§1.530(a) and 1.939(b).</p> <p>B. <input type="checkbox"/> Third party requester in an <i>ex parte</i> reexamination may not file papers in the reexamination file subsequent to the request, except a reply to a proper patent owner statement under 37 CFR 1.530 or a notice of concurrent proceedings as described in MPEP 2282. See 37 CFR §§1.535 and 1.550(g).</p> <p>C. <input type="checkbox"/> Third party requester in an <i>inter partes</i> reexamination may not file papers in the record, except as specified in the rules, 37 CFR §§1.947, 1.951(b) and 1.983, and 37 CFR §§ 41.61-79, other than a notice of concurrent proceedings as described in MPEP 2686. See 37 CFR §1.939.</p> <p>D. <input type="checkbox"/> Parties other than patent owner and a third party requester may not file documents in the record except a notice of concurrent proceedings. See 37 CFR §§1.550(h) and 1.939(a).</p> <p>E. <input type="checkbox"/> The notice of concurrent proceedings exceeds the permitted scope. See MPEP 2282, 2686.</p> <p>F. <input checked="" type="checkbox"/> Other: <u>See attached</u></p> <p>4. CONCLUSION</p> <p style="padding-left: 40px;">Telephone inquiries with regard to this decision should be directed to Mark Reinhart at 571-272-1611, Legal Advisor. In his absence, calls may be directed to Dawn Moore, at 571-272-4587 in the Office of Patent Legal Administration.</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="text-align: center;">  _____ [Signature] </div> <div style="text-align: center;"> Legal Advisor (Title) </div> </div>	

Correspondence in reexamination should identify only the control number assigned. Multiple unrelated control numbers identified on the title page raises confusion as to which proceeding the paper is directed. The only exception permitting multiple control numbers is with merged proceedings in which all merged control numbers are identified on the title page. See MPEP § 2686.01 and 37 C.F.R. §1.989. Reexamination proceedings which are not merged should identify only the control number assigned and no other.

MPEP § 2634 Correspondence (in-part) “After the filing of the request for *inter partes* reexamination, any letters sent to the Office relating to the reexamination proceeding should identify the proceeding by the number of the patent undergoing reexamination, the reexamination request control number assigned, the name of the examiner, and the examiner’s Art Unit.” (emphasis added).

Therefore, the paper filed 05 December 2012 is being expunged from the record.

Note that the re-filed petition dated 11 January 2013, which provides an appropriate header, replaces the earlier filed petition of 05 December 2012.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re <i>Inter Partes</i> Reexamination of:)	
Victor Larson et al.)	Control No.: 95/001,792
U.S. Patent No. 7,188,180)	Group Art Unit: 3992
Issued: March 6, 2007)	Examiner: Deandra M. Hughes
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK)	Confirmation No. 1972
)	<u>VIA EFS WEB</u>

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 CISCO SYSTEMS, INC.'S REVISED PETITION TO
SHORTEN RESPONSE PERIODS AND ACCELERATE PROCEEDINGS**

VirnetX Inc., the owner of the above-referenced patents, opposes third-party requester Cisco Systems, Inc.'s Revised Petition Under 37 CFR § 1.182 to Shorten Response Periods and Accelerate Proceedings ("Petition"). Cisco's dissatisfaction with the progress of the reexaminations is the direct result of Cisco's own delays and strategic decisions during these proceedings. 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. The appropriate \$1930 petition fee under 37 C.F.R. § 1.20(c)(6) was paid in conjunction with VirnetX's Petition in Opposition to Third-Party Requester Cisco Systems, Inc's Petition to Shorten Response Periods and Accelerate Proceedings,

filed December 19, 2012. If any additional fee is due in connection with the filing of this petition, please charge it to Deposit Account 06-0916.

I. Background

A. Control Nos. 95/001,679 and 95/001,682

Cisco 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 Cisco filed Comments on June 14, 2012. The Office merged this proceeding on December 13, 2012 with a separate reexamination involving the ‘135 patent. That other reexamination bears control no. 95/001,682 and names Apple Inc. (“Apple”) as the real party in interest.

B. Control Nos. 95/001,714 and 95/001,697 (“the ‘1,697 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,490,151 (“the ‘151 patent”) on August 16, 2011. The Office granted the Request and ordered reexamination on October 31, 2011. The Office merged this proceeding on March 15, 2012 with a separate reexamination involving the ‘151 patent. That other reexamination bears control no. 95/001,697 and names Apple 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 Cisco filed Comments on August 17, 2012.

C. Control No. 95/001,746 (“the ‘746 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,839,759 (“the ‘759 patent”) on September 7, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on October 14, 2011. Patent Owner timely filed a response to the Office Action on January 17, 2012, and Cisco filed Comments on February 15, 2012.

The Office issued a second Office Action on June 18, 2012. Patent Owner timely filed a response to the second Office Action on August 20, 2012, and Cisco filed Comments on September 18, 2012.

D. Control No. 95/001,792 (“the ’792 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,188,180 (“the ’180 patent”) on October 25, 2011. The Office denied the Request on December 17, 2011. Cisco filed a petition challenging the Office’s denial of the Request on January 17, 2012. The Office granted-in-part Cisco’s petition on September 6, 2012, ordered reexamination, and issued an Office Action on September 19, 2011, which remains pending.

E. Control No. 95/001,851 (“the ’1,851 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,418,504 (“the ’504 patent”) on December 13, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on March 1, 2012. Patent Owner timely filed a response to the Office Action on June 1, 2012, and Cisco filed Comments on June 29, 2012. The Office issued a second Office Action on October 1, 2012, which remains pending.

F. Control No. 95/001,856 (“the ’1,856 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,921, 211 (“the ’211 patent”) on December 16, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on March 5, 2012. Patent Owner timely filed a response to the Office Action on June 5, 2012, and Cisco filed Comments on July 3, 2012. The Office issued a second Office Action on October 1, 2012, which remains pending.

G. Litigation in the Eastern District of Texas

Patent Owner asserted the ’135, ’759, ’180, and ’504 patents in a Complaint filed against Cisco 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 ’151 and ’211 patents in an Amended

Complaint filed against Cisco on April 5, 2011. Cisco and its co-defendant, Apple, filed a sealed motion for separate trials on August 31, 2012. The court granted the motion, set Apple's trial date for October 31, 2012, and set Cisco's trial date for March 11, 2013.

Apple and Patent Owner recently concluded their trial. On November 6, 2012, the jury found the asserted claims of the '135, '151, '504, and '211 patents valid and infringed by Apple, awarding Patent Owner over \$368 million in damages. (Ex. A-10.)

II. Argument

As its trial date approaches, Cisco asserts that the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, 95/001,856 proceedings must be accelerated. (Petition 3.) The primary reasons the reexaminations lag so far behind the district-court action, however, are Cisco's own delays and strategic decisions during these proceedings. The Office should not grant the extraordinary relief sought by Cisco for at least these reasons and for the other reasons discussed below.

First, Cisco did not begin to file these reexamination requests until eleven months after the litigation began, and delayed in some instances for up to sixteen months. Cisco has been on notice of Patent Owner's infringement claims based on the '135, '759, '180 and '504 patents at least since Patent Owner filed its first Complaint on August 11, 2010. Yet Cisco did not file requests for reexamination of the '135, '759, '180 and '504 patents until July 8, 2011, September 7, 2011, October 25, 2011, and December 13, 2011, respectively. Due to Cisco's delays of up to sixteen months in filing, the prosecution of these reexaminations is still before the Central Reexamination Unit. Cisco 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 Cisco. In the 95/001,679, 95/001,714, 95/001,746, 95/001,792,

95/001,851, and 95/001,856 proceedings, Cisco filed enormous requests for reexamination totaling 223, 203, 231, 193, 366, and 366 pages, respectively, including appended claim charts. These requests presented proposed rejections implicating at least 44 different references—several of them well over one hundred pages long. The Office had to review and process all of these papers before issuing Office Actions, and did so within an expeditious timeframe. Cisco could have honed its invalidity positions and filed more targeted reexamination requests to streamline these proceedings, but it did not. Cisco 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 Cisco's vast filings and advancing these reexaminations.

Third, Cisco appears to have been content with the current schedule of the reexaminations throughout their prosecution. Having waited over a year to file many of these reexaminations, Cisco also delayed well beyond the one-year anniversaries of several of these reexamination proceedings before raising any questions regarding the speed of their schedules. (*See id.* at 3.) Cisco's newfound concern, precipitated by its co-defendant Apple's adverse jury verdict and its own now-inconvenient procrastination, does not justify accelerating these proceedings. Doing so would only further burden the Patent Owner and the Office when the Office is already responding with "special dispatch" to the enormous number of issues raised in Cisco's lengthy and late-filed reexamination requests.

Fourth, accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would also substantially prejudice Patent Owner. Along with these proceedings, Patent Owner is concurrently involved in five additional reexaminations naming Apple as the real party in interest, which are also demanding significant attention from Patent Owner. (*See* control nos. 95/001,682; 95/001,788; 95/001,789; and 95/001,949 and the merged proceedings in control nos. 95/001,697 and 95/001,714.) Accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would therefore unreasonably burden Patent

Owner and its counsel. Patent Owner would not have sufficient time and opportunity to respond adequately within shortened time periods, given that it must also respond to filings from Apple in a large number of other reexaminations. Indeed, Patent Owner recently prepared responses to *five* concurrently pending Office Actions. (See control nos. 95/001,788; 95/001,789; 95/001,792; 95/001,851; and 95/001,856).

Finally, shortening Patent Owner's response periods would not achieve any benefit in these proceedings. Cisco vaguely asserts that "[q]uickly reaching a final decision on the invalidity of the patents in reexamination . . . will ensure that the outcomes of the Office proceedings will be considered in conjunction with related proceedings." (Petition 2.) But if Cisco is referring to the litigation as the "related proceedings," the district court in fact will enter a final judgment and the litigation will reach the Federal Circuit long before the reexaminations will, given the upcoming trial date of March 11, 2013. Thus, even if the Office were to grant Cisco's request (which it should not), the reexaminations will not be ready for appeal to the Federal Circuit for quite some time. Because the relief requested will not help to align the litigation and the reexaminations, and because Cisco is seeking relief from the consequences of its own strategic decisions, shortening Patent Owner's response periods to respond to the enormous number of issues raised in Cisco's lengthy reexamination requests would be unreasonable and prejudicial.

III. Conclusion

The reexaminations are proceeding with the appropriate "special dispatch." Cisco's complaints arise chiefly from its own delay in waiting to file its requests for reexamination, as well as from its own strategic decisions during the course of these reexaminations. Moreover, the relief requested would not promote efficiency, but rather would only prejudice the Patent Owner. Indeed, hurried prosecution of these proceedings would likely result in incomplete consideration of the issues

and in fact act to slow the reexaminations. In view of all of the foregoing circumstances, Patent Owner respectfully submits that Cisco's petition should be denied.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 17, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re <i>Inter Partes</i> Reexamination of:)	
)	Control No.: 95/001,792
Victor Larson et al.)	
)	Group Art Unit: 3992
U.S. Patent No. 7,188,180)	
)	Examiner: Deandra M. Hughes
Issued: March 6, 2007)	
)	Confirmation No. 1972
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 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 Cisco Systems, Inc.'s Revised Petition to Shorten Response Periods and Accelerate Proceedings was served by first-class mail on January 17, 2013, on counsel for the third party requester at the following address:

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: January 17, 2013

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14726534
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	17-JAN-2013
Filing Date:	25-OCT-2011
Time Stamp:	14:47:06
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		05Petition.pdf	369138 <small>feb691c8b0ea2409395fbc707db15fcc8af17759</small>	yes	8

Multipart Description/PDF files in .zip description		
Document Description	Start	End
Reexam Miscellaneous Incoming Letter	1	7
Reexam Certificate of Service	8	8
Warnings:		
Information:		
Total Files Size (in bytes):		369138
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>		

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Reexamination Control No.: 95/001,792	§	Attorney Docket No.: 43614.100
	§	
Patent No.: 7,188,180	§	Customer No.: 27683
	§	
For: METHOD FOR ESTABLISHING	§	Real Party In Interest:
SECURE COMMUNICATION LINK	§	Cisco Systems, Inc.
BETWEEN COMPUTERS OF VIRTUAL	§	
PRIVATE NETWORK	§	
	§	
Examiner: Deandra M. Hughes	§	
	§	
Art Unit: 3992	§	Conf. No. 1972

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

Dear Sir:

On December 19, 2012, the Patent Owner filed the Patent Owner's Response to Office Action ("Response") for the Office Action mailed September 19, 2012 ("Office Action") in connection with the above-identified *inter partes* reexamination proceeding.

It is respectfully requested, for the reasons identified below, that the Examiner:

- (i) maintain the rejection of, and issue an action closing prosecution for, original claims 1, 4, 6-17, 20, 22-33, 35 and 37-41 (all of the claims subject to reexamination), and
- (ii) deem the arguments advanced by the Patent Owner in the Response to be erroneous, improper, and/or unpersuasive.

In the context of this *inter partes* reexamination, the standard provided in MPEP § 2111 for claim interpretation during patent examination is applied.

TABLE OF CONTENTS

I.	REPLY TO PATENT OWNER ARGUMENTS.....	1
A.	The Rejection of Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, 39, and 40 Under 35 USC § 102(b) Based On Kiuchi Were Proper	1
1.	Independent Claim 1	1
2.	Independent Claims 17 and 33.....	6
3.	Dependent claims 6, 22 and 37	6
4.	Dependent Claims 8, 24 and 39	8
5.	Dependent Claims 9, 25, and 40	9
6.	Dependent claims 12 and 28	10
7.	Dependent Claims 13, 15, 29 and 31	12
8.	Dependent Claims 16 and 32	12
9.	Dependent claims 4, 10, 14, 20, 26, 30 and 35	12
B.	The Rejection of Claims 11, 27 And 41 Under 35 USC § 103 Based On Kiuchi Were Proper	13
C.	The Rejection of Claims 7, 23 and 38 Under 35 USC § 103 Based On Kiuchi in View of Martin Were Proper	14
D.	Response to Patent Owner’s Argument That Secondary Considerations Demonstrate Non-Obviousness	15
II.	CONCLUSION.....	17

LIST OF EXHIBITS

The present comments by third party requester are accompanied by the following reference materials that, pursuant to 37 CFR 1.943, are excluded from the page limit restrictions.

- Exhibit F¹: Joint Claim Construction Chart for US 7,188,180, *VirnetX v. Cisco*, No. 6:10-cv-00417, Docket No. 194 (Dec. 21, 2011) (selected pages).
- Exhibit G: U.S. Patent No. 5,706,218
- Exhibit H: Excerpt from Microsoft Computer Dictionary, Fourth Edition
- Exhibit I: Excerpt from *A First Course in Probability, Sixth Edition*, Sheldon Ross

¹ Exhibits A-E are part of the originally filed Request for Reexamination.

I. REPLY TO PATENT OWNER ARGUMENTS

A. The Rejection of Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, 39, and 40 Under 35 USC § 102(b) Based On Kiuchi Were Proper

1. Independent Claim 1

a. Kiuchi Discloses “Sending an Access Request Message ... Using a Virtual Private Network Communication Link”

On pages 5-7, Patent Owner argues Kiuchi does not disclose “sending an access request message ... using a virtual private network communication link.” Patent Owner focuses on the steps in Kiuchi that must occur before a connection is established between the client-side proxy and the server-side proxy. Then, Patent Owner concludes that Kiuchi’s request for connection is not using a virtual private network communication link, because the C-HTTP connection between the client-side proxy and server-side proxy has not been established, and that the link used for sending the access request message “lacks the requisite features of a virtual private network communication link.” Patent Owner’s arguments are not persuasive.

First, Patent Owner is attempting to improperly import limitations into the claims. Patent Owner argues that the link used to send the access request message of Kiuchi does not have the “requisite features” of a virtual private network and is a “mere point-to-point communication.” Patent Owner also argues that the two computers of Kiuchi are not connected via a virtual private network communication link because the two computers are not connected within the same network. This is improper. The language of the claims contains no limitations about “not communicating via point-to-point communication” or that the computers must be “connected within the same network.” The claims simply recite “sending an access request message ... using a virtual private network communication link.” The limitations relied upon by the Patent Owner (“no point-to-point communication” and “connected within the same network”) are not recited in the claims, and therefore do not differentiate over Kiuchi.

Second, Patent Owner’s own statements and admissions show Kiuchi teaches this limitation. Patent Owner has previously stated that a “virtual private network” is a “network of computers which privately communicate with each other by encrypting traffic on insecure

communications paths between the computers.”² Patent Owner’s statements do not reference or require “not communicating via point-to-point communication” or “computers connected within the same network.” Applying Patent Owner’s definition, Kiuchi teaches the claim limitation. When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, the client-side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy’s public key. (Kiuchi at p. 65).

Patent Owner’s Claim Construction	Kiuchi at p. 65
network of computers which privately communicate with each other	Kiuchi teaches a private, closed members-only network: “When the C-HTTP name server confirms that the specified server-side proxy is an <i>appropriate closed network member...</i> ”
by encrypting traffic on insecure communications paths between the computers	Kiuchi teaches that the connection request is encrypted: “...a client-side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy’s public key.”

Accordingly, not only does Kiuchi teach “sending an access request message ... using a virtual private network communication link” as interpreted by the Examiner, Kiuchi teaches the claim, *as construed by the Patent Owner*.

The Examiner’s rejection was proper and should be maintained.

b. Kiuchi Discloses “the Query Message Requesting From the Secure Domain Name Service a Secure Computer Network Address Corresponding to the Secure Domain Name”

On pages 7-9, Patent Owner argues that Kiuchi does not teach “the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” Patent Owner states that in Kiuchi’s system, a client would send a query with the domain name of an origin server and receive in response the IP

² Exhibit F, Patent Owner’s proposed claim construction for “virtual private network.”

address for a server-side proxy. Thus, Patent Owner asserts that Kiuchi's domain names and the returned IP addresses do not "correspond." Patent Owner's argument is without merit.

Interpreting claims to exclude disclosed embodiments in the specification is routinely improper. *See, e.g., Verizon Servs. Cop v. Vonage Holdings corp.*, 503 F.3d 1295, 1305 (Fed. Cir. 2007). In this instance, claim 1 is silent as to the nature of the "correspond[ence]." Moreover, the '180 patent's specification describes embodiments having only a loose correspondence between the requested domain name and the corresponding IP address that is returned. For example:

- "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*)" ('180 Patent, 40:59-63, emphasis added); and
- "The address that is returned *need not be the actual address* of the destination computer" ('180 Patent, 40:63-64, emphasis added).

Thus, the specification contemplates embodiments where the IP address that is returned need not be the actual address of the target computer. Therefore, Patent Owner's purported distinction over Kiuchi (that Kiuchi does not teach returning the actual address of the target computer) is excluding specific embodiments disclosed in the specification.

Further, even if the Examiner adopted the Patent Owner's argument (that the claims require that the IP address must be the address for the domain name), Kiuchi nevertheless teaches "a secure computer network address corresponding to the secure domain name."

Kiuchi teaches that the client-side proxy sends a secure domain name to the C-HTTP name server (the secure domain name service). In response, the C-HTTP name server transmits to the client-side proxy an IP address:

2) Lookup of server-side proxy information (Appendix 3. a,b)

A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values. If it is not permitted, it sends a status code which indicates an error.

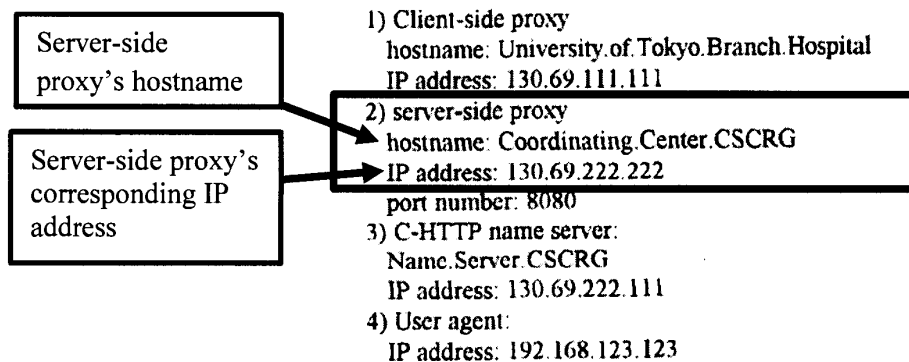
(Kiuchi at p. 65).

Patent Owner argues that the IP address returned by the name server corresponds only to the server-side proxy, and thus does not correspond to the *host* specified in a given URL. However, Patent Owner ignores the example in “Appendix 3.a,b” of Kiuchi, where Kiuchi *expressly teaches* an embodiment in which the IP address returned by the nameserver is the IP address that *directly corresponds* to the hostname contained in the query message.

Turning the example in Appendix 3 of Kiuchi, Kiuchi shows the “components of C-HTTP-based communication.” One of the components is a “server-side proxy” that has (i) a hostname (Coordinating.Center.CSCRG) and (ii) a corresponding IP address (130.69.222.222):

Appendix 3. Examples of C-HTTP communication (a-h)

Note that lines with an asterisk are encrypted. Components of C-HTTP-based communication are as follows:



Then, in step “a,” Kiuchi performs a “lookup of server-side proxy information” by transmitting a hostname to the C-HTTP name-server:

a. Lookup of server-side proxy information (C-HTTP name service protocol)

Server-side proxy's hostname sent in the query to the C-HTTP name server

```
C-HTTPNS/0.1<CR><LF>
RSA<CR><LF>
74<CR><LF>
RSA<CR><LF>
32<CR><LF>
MD5<CR><LF>
<CR><LF>
*SERVER<CR><LF>
*130.69.111.111<CR><LF>
*192.168.123.123<CR><LF>
*Coordinating.Center.CSCRG<CR><LF>
*8080<CR><LF>
<CR><LF>
*827ae79ba214769ea2998249bdb9aa97
```

In step “b,” the C-HTTP name server of Kiuchi responds with the IP address corresponding to the hostname:

b. Response from the C-HTTP name server, indicating that the connection is permitted (C-HTTP name service protocol)

IP address transmitted back. (this IP address corresponds to the hostname “Coordinating.Center.CSCRG”, as shown above)

```
RSA<CR><LF>
203<CR><LF>
RSA<CR><LF>
32<CR><LF>
MD5<CR><LF>
<CR><LF>
*OK<CR><LF>
*130.69.111.111<CR><LF>
*192.168.123.123<CR><LF>
*130.69.222.222<CR><LF>
*8080<CR><LF>
*effe0d7f480dad7cbbe9d0c309b2f04c89fe5e8e9f7bfc1854
b62f6b4bafa981c1a64e19fd6c702cec376f9dea4f5422e851
bb1770ce600d246637459ab757b<CR><LF>
*8abd853f<CR><LF>
*ef23dc99<CR><LF>
*<CR><LF>
<CR><LF>
*51a2f15a51a7f64a5ada6ac40bc529ba
```


Since Kiuchi specifically teaches an embodiment in which a hostname directly corresponds to the server-side proxy, and the hostname is used to retrieve the IP address corresponding to the hostname, Patent Owner's attempted distinction over Kiuchi is incorrect and without merit.

Accordingly, Patent Owner has attempted to improperly interpret the claim to exclude embodiments described in the specification, while also ignoring the full teachings of Kiuchi. The Examiner's rejection was proper and should be maintained.

2. Independent Claims 17 and 33

On page 9, Patent Owner makes no additional arguments with respect to claims 17 and 33, other than to cross-reference back to claim 1. For the reasons set for above, claims 17 and 33 are anticipated by Kiuchi. Since Patent Owner makes no additional arguments, the Examiner's rejections of claims 17 and 33 are proper and should be maintained.

3. Dependent claims 6, 22 and 37

First, Patent Owner argues on page 9 that claims 6, 22 and 37 depend from independent claims 1, 17 and 33 and includes all of the features of those claims. For the reasons set for above, claims 1, 17 and 33 are anticipated by Kiuchi.

Second, Patent Owner argues on page 9 that Kiuchi does not disclose "the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network." Patent Owner is incorrect.

Kiuchi discloses "the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network," because Kiuchi discloses inserting version information into the request ("C-HTTP-Version = 'C-HTTP/0.7'") and into the response ("C-HTTP-Version-Line = 'C-HTTP/0.7'") (Kiuchi at 70, 71). The C-HTTP version value inserted into the request and the response defines the "version of C-HTTP name service protocol" being used. (Kiuchi at 72). The version of the name service protocol is a data value representing a predetermined level of service.

Accordingly, because Kiuchi inserts version information defining the name service into each request and response, Kiuchi discloses “the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.”

Patent Owner argues on page 9 that an anticipation rejection cannot rely on multiple references, and argues that Requester has neither shown nor attempted to show that Kiuchi’s C-HTTP system would necessarily insert into at least one data packet at least one data value representing a predetermined level of service. Patent Owner’s argument is without merit.

Kiuchi specifically teaches that (i) the C-HTTP name service protocol sends the version information for the name service and (ii) the communication occurs over a TCP/IP session. Patent Owner argues that the Examiner has neither shown nor attempted to show that Kiuchi’s C-HTTP system would necessarily insert into at least one data packet at least one data value representing a predetermined level of service. Patent Owner is incorrect. Kiuchi specifically teaches that each response and each request require version information that define the C-HTTP service. (Kiuchi at 70, 71) Further, explicit disclosures are not required and the prior art is not to be considered in a vacuum but, “together with the knowledge of one of ordinary skill in the pertinent art...at the time the...patent was filed.” *In re Paulson*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). *See also, In re Baxter Travenol Labs*, 952 F.2d 388, 391 (Fed. Cir. 1991).

RFC 793 was provided to show the knowledge of one of ordinary skill at the time. Per RFC 793, a TCP/IP session “makes use of the internet protocol *type of service field* and security option to provide precedence and security on a per connection basis to TCP users.” (RFC 793 at p. 12, emphasis added). Accordingly, when Kiuchi is viewed with the knowledge of one of ordinary skill in the art (e.g., a basic understanding of the TCP/IP session used in Kiuchi), it is clear that Kiuchi used TCP, which uses a “type of service” field to provide a predetermined level of service.

Third, Patent Owner argues that the Examiner has not shown any “nexus” between service fields and the C-HTTP connection. Patent Owner’s argument is without merit. Kiuchi specifically states that *each* request and *each* response that establish the C-HTTP connection use the service field (e.g., the version of the service protocol). Patent Owner points to no claim language requiring any “nexus” or any other special relationship between the at least one data value and the virtual private network. Kiuchi discloses that the C-HTTP connection is

established by a request and a response, where each request and response contains a data value that indicates the particular version of C-HTTP being used to establish the connection.

The Examiner's rejection was proper and should be maintained.

4. Dependent Claims 8, 24 and 39

First, Patent Owner argues on page 10 that claims 8, 24 and 39 depend from independent claims 1, 17 and 33 and includes all of the features of those claims. For the reasons set for above, claims 1, 17 and 33 are anticipated by Kiuchi.

Second, Patent Owner argues on page 10 that Kiuchi does not disclose that “the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.” Patent Owner is incorrect.

Kiuchi discloses a “moving window of valid values” because the Nonce values of Kiuchi are values that indicate where a packet belongs in a message sequence, and the Nonce values are checked to prevent attacks. Kiuchi discusses an example sequence involving a number of requests and responses. Within those requests and responses are the Nonce values. Those Nonce values from those requests and responses are reproduced below:

Request-Nonce	Response-Nonce
8abd853f	ef23dc99
8abd8540	ef23dc9a
8abd8541	ef23dc9b

(See Kiuchi, 74-75)

Patent Owner argues that the Nonce values are not compared against a moving window of valid values and that Kiuchi does not explain how the values are checked. Patent Owner's arguments contradict the specification of the '180 patent. The specification defines a “moving window of valid values”: “1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.” ('180 Patent, 11:59-61). Since Kiuchi checks for Nonce values for the correct sequence (e.g., incrementing “853f...8540...8541” and “c99...c9a...c9b”), then Kiuchi is comparing a value in each message (the Nonce value) to a moving window of valid values (an identifier indicating where the message belongs in the message sequence).

Accordingly, (i) Kiuchi discloses an identifier that indicates where the packet belongs in the message sequence, and (ii) the specification of the '180 patent defines a window sequence number as an identifier that indicates where the packet belongs in the original message sequence. Thus, the identifiers of Kiuchi that indicate the message sequence are a "moving window of valid values."

Third, Patent Owner argues on page 10 that the C-HTTP requests and responses may contain Nonce values, but that the Nonce values are not inserted into "each data packet." Patent Owner's argument is without merit. The claims recite "each data packet." However, the specification mentions many types of packets: "TARP packets," "data packets," "IP packets" ('180 at 11: 29-58), "decoy packet" ('180 Patent, 16: 23), "secure synchronization request packet" ('180 Patent, 18: 20-21), "response packet" ('180 Patent, 18: 36), "ACK packet" ('180 Patent, 18: 37), "secure session initiation packet" ('180 Patent, 18: 41-42), and "SYNC_REQ packet" ('180 Patent, 30: 7-8). Notably, the claims do not recite any particular type of packet, size of packet, or type of communication protocol for sending the packet – the claims merely recite "data packet." If the Patent Owner wanted the claim limited to only "IP packet" or "ACK packet," those terms should be recited in the claims. To the contrary, there is nothing in the claims or the specification to suggest that "data packets" have such a limited definition, and thus, Patent Owner is improperly importing limitations into the "data packets" recited in the claims. Under the broadest reasonable interpretation of "data packet," the packets of data that form the C-HTTP request and the C-HTTP response of Kiuchi teach and disclose "each data packet."

5. Dependent Claims 9, 25, and 40

First, Patent Owner argues on page 11 that claims 9, 25 and 40 depend from independent claims 1, 17 and 33 and includes all of the features of those claims. For the reasons set for above, claims 1, 17 and 33 are anticipated by Kiuchi.

Second, Patent Owner argues on page 11 that the connection ID in Kiuchi does not disclose a "discriminator field" because the connection ID is not in "each data packet." Again, Patent Owner's argument is without merit. The claims recite "each data packet." However, the specification mentions many types of packets: "TARP packets," "data packets," "IP packets" ('180 Patent, 11: 29-58), "decoy packet" ('180 Patent, 16: 23), "secure synchronization request

packet” (‘180 Patent, 18: 20-21), “response packet” (‘180 Patent, 18: 36), “ACK packet” (‘180 Patent, 18: 37), “secure session initiation packet” (‘180 Patent, 18: 41-42), and “SYNC_REQ packet” (‘180 Patent, 30: 7-8). Notably, the claims do not recite any particular type of packet, size of packet, or type of communication protocol for sending the packet – the claims merely recite “data packet.” If the Patent Owner wanted the claim limited to “IP packet” or “ACK packet,” those terms should be recited in the claims. To the contrary, there is nothing in the claims or the specification to suggest that “data packets” have such a limited definition. Patent Owner is improperly importing limitations into the “data packets” recited in the claims. Under the broadest reasonable interpretation of “data packet,” the packets of data that form the C-HTTP request and the C-HTTP response of Kiuchi teach and disclose “each data packet.”

Third, Patent Owner argues that Kiuchi does not teach that the virtual private network of Kiuchi *is based* on a comparison of a discriminator field. There is nothing recited in the claims about what type of comparison is performed against the “table of valid discriminator fields.” Further, Kiuchi discloses that the check of the connection ID against a connection table is a necessary step for the formation of the virtual private network: “When the connection ID is not found in the current connection table in the client-side- proxy, the current connection is disconnected” (Kiuchi at p. 65). Accordingly, Kiuchi discloses that the connection ID is compared against a table of current connections, and if the connection ID is not found, then the connection is disconnected. Accordingly, Kiuchi discloses that the virtual private network is *based on* a comparison of the discriminator field (e.g., the connection ID) in a header of each data packet (e.g., the C-HTTP response and C-HTTP request) to a table of valid discriminator fields (e.g., the current connection table).

The Examiner’s rejection was proper and should be maintained.

6. Dependent claims 12 and 28

First, Patent Owner argues on page 11 that claims 12 and 28 depend from independent claims 1 and 17 and includes all of the features of those claims. For the reasons set for above, claims 1, 17 and 33 are anticipated by Kiuchi.

Second, Patent Owner argues on page 12 that the connection ID and symmetric data exchange key are not *stored* at the secure computer network address, but are newly generated.

Patent Owner concludes, then, that the access request message cannot contain a request for information stored at the server, because that information is not generated at the time the access request message is sent. Patent Owner's argument is without merit.

The claims do not recite *when* the information must be stored. There is nothing recited in the claims that limits the claims to only information stored *before* the access request message is transmitted. In Kiuchi, the access request message is requesting the connection ID from the server-side proxy. The connection ID (e.g., the information requested) is generated and then stored at the secure computer network address (e.g., the server-side proxy), because Kiuchi teaches that server-side proxy needs to delete the connection ID after the connection is closed (i.e., in order for it to be deleted, the connection ID must have first been stored).

Further, to the extent that the claim is nevertheless interpreted to require that the information requested by the access request message must exist at the time the message is sent, Kiuchi also teaches that the server side proxy ip and server side proxy name, which exist before the access request message is sent, are returned in response to the access query message:

f. Response from the server-side proxy, indicating that the connection is established

```
C-HTTP/0.7<CR><LF>
Encryption-Algorithm: RSA<CR><LF>
Encrypted-Header-Length: 341<CR><LF>
Signature-Algorithm: RSA<CR><LF>
Signature-Length: 32<CR><LF>
Message-Digest-Algorithm: MD5<CR><LF>
<CR><LF>
*Status: 200 OK<CR><LF>
*Server-Side-Proxy-IP: 130.69.222.222<CR><LF>
*Server-Side-Proxy-Name:
Coordinating Center CSCRG<CR><LF>
*Server-Side-Proxy-Port: 8080<CR><LF>
*Client-Side-Proxy-IP: 130.69.111.111<CR><LF>
*Client-Side-Proxy-Name:
University of Tokyo.Branch.Hospital<CR><LF>
*User-Agent-IP: 192.168.123.123<CR><LF>
*Connection-ID: 6zdDfIdfcZLj8V!i<CR><LF>
*Response-Nonce: ef23dc99<CR><LF>
*Response-Data-Exchange-Key: a-3f(*d.bfs,<CR><LF>
<CR><LF>
*36e2bfc5022208ca8c20307f60d15e2e
```

Server side proxy ip address and server side proxy name are included in the response from the server-side proxy.

(Kiuchi at pg. 74)

Accordingly, not only does Kiuchi teach that the server side proxy stores the connection ID, but also teaches that the server side proxy stores its IP address and hostname. Thus, Kiuchi discloses “wherein the access request message contains a request for information stored at the secure computer network address.”

7. Dependent Claims 13, 15, 29 and 31

First, Patent Owner argues on page 12 that claims 13, 15, 29 and 31 depend from independent claims 1 and 17 and includes all of the features of those claims. For the reasons set for above, claims 1, 17 and 33 are anticipated by Kiuchi.

Second, Patent Owner argues that Kiuchi does not disclose that the claimed methods occur at, or are performed by, a “client computer” because a “person of ordinary skill at the time of the invention would have been readily capable of distinguishing, as *Kiuchi* does, between client computers within an institutional firewall (e.g., a nurse’s or doctor’s PC in a hospital) and a computer residing on an institutional firewall (e.g., a client-side proxy)” (Response at pp. 12-13). But, Patent Owner’s argument *establishes that Kiuchi teaches the claim limitations*.

Kiuchi teaches a user agent that communicates with a client-side proxy. A user enters a hostname into the user agent (e.g., a nurse’s PC in a hospital), which sends the hostname to the client-side proxy. Accordingly, the client-side proxy receives the hostname and the hostname was from the user. Thus Kiuchi discloses the method occurring at and being performed by a client computer.

8. Dependent Claims 16 and 32

Patent Owner notes that claims 16 and 32 depend from claims 2 and 18. However, Patent Owner provides no argument rebutting the finding Kiuchi discloses “wherein receiving the command comprises receiving the command at a client computer from a user.”

9. Dependent claims 4, 10, 14, 20, 26, 30 and 35

On page 13, Patent Owner argues that Kiuchi does not anticipate claims 4, 10, 14, 20, 26, 30 and 35 because claims 4, 10, 14, 20, 26, 30 and 35 depend from independent claims 1, 17 and

33. For the reasons already set forth above, Kiuchi does, in fact, anticipate claims 1, 17 and 33. Thus, because Patent Owner has made no other arguments specific to the limitations of claims 4, 10, 14, 20, 26, 30 and 35, Patent Owner has not rebutted Patent Office's rejection of claims 4, 10, 14, 20, 26, 30 and 35.

B. The Rejection of Claims 11, 27 And 41 Under 35 USC § 103 Based On Kiuchi Were Proper

On pages 13-14, Patent Owner argues that adding a letter "s" to the known top-level domain names of .com, .net, .org, .edu and .gov is not obvious to a person of ordinary skill in the art. Patent Owner argues that the Examiner provided no "articulated reasoning" to support the obviousness rejection.

The Examiner showed that (i) Kiuchi teaches secure domain names that correspond to conventional domain names; and (ii) .com, .net, .org, .edu and .gov are known character combinations used to represent top level domain names. Since it was known in the art that character combinations can be used to represent top level domain names, mere design choice is "an acceptable rationale for an obviousness rejection when a claimed product merely arranges known elements in a configuration recognized as functionally equivalent to a known configuration." *See, Ex parte Gunasekar*, Appeal 2009-008345 in 10/903,590 (BPAI 2011). Rearranging letters is a mere design choice.

Further, Patent Owner argues that nothing in Kiuchi would disclose "modifying a top-level domain name to denote security." Once again, Patent Owner attempts to introduce limitations into the claims. The claims recite nothing about "denoting security." The claims simply recite a list of letters as possible top-level domain names, which is merely a design choice rearranging known elements.

The Examiner's rejection was proper and should be maintained.

C. **The Rejection of Claims 7, 23 and 38 Under 35 USC § 103 Based On Kiuchi in View of Martin Were Proper**

The Examiner properly rejected claim 7, 23, and 38 because: (i) Kiuchi teaches a virtual private network established over the Internet between two computing devices (Kiuchi at 64); and (ii) Martin teaches a known technique of a computer address hopping regime using randomly chosen network addresses for Internet (TCP) communication. In particular, Martin discloses that an “outbound TCP connection should select its source address/port pair from A_{TCP} at random.” (Martin at 9, emphasis added).

Accordingly, the prior art teaches that when a client is initiating a new communication link to a server, the client can randomly choose both the source (“from”) address and the destination (“to”) address to be used. The addresses used can be different for each connection. Thus, the prior art teaches a “network address hopping regime that is used to pseudorandomly change network addresses in packets” as recited in the claims.

The Patent Owner argues, without explanation, that a regime for changing network addresses based on randomly selecting source and destination addresses, as taught by Kiuchi and Martin, is somehow different than “pseudorandomly³ chang[ing] network addresses in packets”

³ It is well-known in the computer science art that the term “random” is understood to mean “pseudo random.” Evidence of such well-known art can be found in:

- Patents, such as U.S. Patent No. 5,706,218 (“Circuits for generating random numbers, or more accurately, pseudo random numbers are well-known in the art”) (Ex. G);
- Technical dictionaries, such as the Microsoft Computer Dictionary, Fourth Edition (“**random number generation** *n.* Production of an unpredictable sequence of numbers ... Truly random number generation is generally viewed as impossible. The process used in computers would be more properly called ‘pseudorandom number generation’.”) (Ex. H); and
- Textbooks, such as *A First Course in Probability, Sixth Edition* (“In order to use a computer to initiate a simulation study, we be able to generate the value of a uniform (0,1) random variable; such variates are called random numbers. To generate such numbers, most computers have a built-in subroutine, called a random number generator, who output a sequence of pseudo random numbers.”) (Ex. I).

Thus, a person of ordinary skill in the art, when reading Martin, would understand that the “random” in Martin is pseudo-random, because Martin is a discussion about computer

as recited in the claims. Randomly using different network addresses for each connection as taught by the combination of Kiuchi and Martin teaches that the source and destination network addresses in the packets transiting the virtual private network randomly change. To the extent that the Patent Owner believes that the claim has a different meaning, the Patent Owner has neither explained that meaning nor provided any reasoning for it. (See 37 CFR 1.111(b).)

The rejections were proper and should be maintained.

D. Response to Patent Owner's Argument That Secondary Considerations Demonstrate Non-Obviousness

On pages 15-17, Patent Owner argues that secondary considerations rebut any finding of obviousness. To be given substantial weight in determining obviousness or nonobviousness, evidence of secondary considerations must be relevant to the subject matter as claimed, and therefore the Examiner must determine whether there is a nexus between the merits of the claimed invention and the evidence of secondary considerations. MPEP 716.01(b). Further, in the absence of an established nexus with the claimed invention, secondary consideration factors are not entitled to much, if any, weight and generally have no bearing on the legal issue of obviousness. *See In re Vamco Machine & Tool, Inc.*, 752 F.2d 1564, 1577 (Fed. Cir. 1985).

First, Patent Owner has failed to establish any nexus between the '180 patent and the "evidence." Patent Owner points to a declaration by the inventor of the '180 that describes different government funding programs designed to promote science and technology. However, simply because a government agency funds research programs for "Information Assurance," "Dynamic Coalitions, and "Next Generation Internet" does not establish a nexus between those programs and the actual claims of the '180 patent. In order for any such evidence to be given weight, if any, the Patent Owner must establish a nexus between the evidence and the claimed invention. Patent Owner has merely listed a number of government-funded programs, with a passing reference to "secure communications." Patent Owner has not established a nexus between this evidence **and the actual claims of the '180 patent.**

networking (i.e., the "random" taught in Martin is generated by a computer, and is thus actually pseudo-random).

Second, Patent Owner argues that the claimed invention has achieved commercial success by noting that several companies have licensed the patent portfolio. However, **a portfolio license does not establish commercial success.** (*Ex parte NTP, Inc., Appeal 2008-004603, slip op. at 132 (BPAI Dec. 22, 2009)*). The Board of Patent Appeals and Interferences has set forth the evidence needed to support the use of a list of licensees as evidence of secondary considerations: (i) testimony from a licensee as to why the licensee took a license; (ii) whether the taking of the license was a business cost-benefit analysis with regarding to defending an infringement suit, as opposed to the actual merits of the invention; (iii) the number of entities who refused to take a license and why; (iv) the terms of the licenses and whether the licenses were favorable to the licensee; (v) market information indicating the number of products that are sold under licenses and the number of products that are not under license; (vi) the structure and operation of the devices made by the licensees to determine if those products embody the reasons as to why the “invention” is advantageous over the prior, if at all; (vii) whether the licensee took the licenses for reasons substantively related to each and every one of the claims of the ‘180 patent; and (viii) a declaration from a representative of any of the licensees attesting to and praising the merits of the claimed invention. (*Ex parte NTP at 132-134*). Patent Owner has not provided any such evidence. Patent Owner has not carried the burden of demonstrating that the “evidence” has any bearing on nonobviousness.

Accordingly, the evidence of secondary considerations should be afforded no weight. The Examiner’s rejections based on obviousness were proper.

II. CONCLUSION

Therefore, it is requested that rejections in the Office Action be maintained.

As identified in the attached Certificate of Service and in accordance with MPEP §2266.06 and 37 CFR §§1.248 and 1.903, a copy of the present response, in its entirety, is being served to the address of the attorney/agent of record at the address provided for in 37 CFR 1.33(c). Please direct all correspondence in this matter to the undersigned.

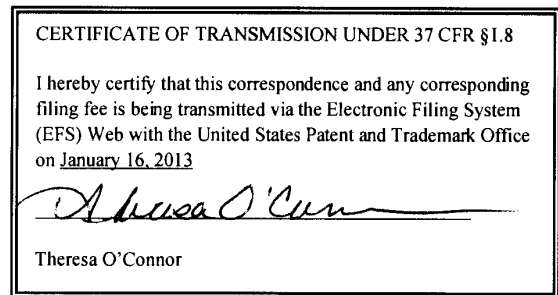
Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: January 16, 2013

HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Attorney Docket No.: 43614.100



CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the following:

Comments by Third Party Requester Pursuant To 37 C.F.R. §1.947 and Exhibits F-I in their entirety were served on:

Finnegan, Henderson, Farabow, Garrett & Dunner LLP
901 New York Avenue, NW
Washington DC 20001-4413

the attorneys identified in the Power of Attorney and who filed the Patent Owner's Response to Office Action, on January 16, 2013.

/David L. McCombs/

David L. McCombs, Registration No. 32,271

Electronic Acknowledgement Receipt

EFS ID:	14717954
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	16-JAN-2013
Filing Date:	25-OCT-2011
Time Stamp:	16:55:43
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		3PR_Comments_COS.pdf	973020 <small>28fa92b10545009da98eb29269869da1c6c26fc9</small>	yes	21

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Third Party Requester Comments after Non-final Action			1	20	
Reexam Certificate of Service			21	21	
Warnings:					
Information:					
2	Reexam Miscellaneous Incoming Letter	Ex_F_Joint_Claim_Construction_Excerpt.pdf	1631562	no	7
			<small>f2ca1d1774b7d1ce2690f58448ca33e3cd23f009</small>		
Warnings:					
Information:					
3	Reexam Miscellaneous Incoming Letter	Ex_G_US5706218.pdf	1448112	no	7
			<small>bb4b49090b3fa7c909704f00050726c3873e4740</small>		
Warnings:					
Information:					
4	Reexam Miscellaneous Incoming Letter	Ex_H_MS_Comp_Dict.pdf	2884193	no	4
			<small>4933f312b7adbdcf764e3a7a0d144eacc65a5cc7</small>		
Warnings:					
Information:					
5	Reexam Miscellaneous Incoming Letter	Ex_I_Probability.pdf	1859991	no	5
			<small>c03f3fb7af52957c63c3599f981a1b11267849cd</small>		
Warnings:					
Information:					
Total Files Size (in bytes):			8796878		

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

Reexamination Control No.: 95/001,792	§	Attorney Docket No.: 43614.100
	§	
Patent No.: 7,188,180	§	Customer No.: 27683
	§	
For: METHOD FOR ESTABLISHING	§	Real Party In Interest:
SECURE COMMUNICATION LINK	§	Cisco Systems, Inc.
BETWEEN COMPUTERS OF	§	
VIRTUAL PRIVATE NETWORK	§	
	§	
Examiner: Deandra M. Hughes	§	Conf. No. 1972
	§	
Art Unit: 3992	§	

Mail Stop: Petition
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

**REVISED PETITION UNDER 37 CFR § 1.182 TO
SHORTEN RESPONSE PERIODS AND ACCELERATE PROCEEDINGS**

I. Introductory Remarks

Requester hereby petitions under the provisions of 37 C.F.R. § 1.182 to request that the Patent Office accelerate and bring to a close the various long-pending reexaminations, including setting shortened statutory periods for future Patent Owner responses. Quickly reaching a final decision on the invalidity of the patents in reexamination (now pending for over a year) will ensure that the outcomes of the Office proceedings will be considered in conjunction with related proceedings.

In accordance with 37 C.F.R. § 1.20(c)(6), the petition fee of \$1930.00 was paid with the Third Party Requester's Petition to Shorten Response Periods and Accelerate Proceedings filed previously on December 5, 2012. The Commissioner is hereby authorized to charge any deficiency or credit any overpayment for this request to Deposit Account No. 08-1394.

II. Statement of Facts

The pertinent facts are as follows:

- Patent Owner owns U.S. Patent No. 6,502,135, U.S. Patent 7,490,151, U.S. Patent 7,418,504, U.S. Patent No. 7,921,211, U.S. Patent 6,839,759, U.S. Patent 7,188,180, and U.S. Patent 8,051,181.
- Each of those patents claims priority to, *inter alia*, U.S. Provisional Application No. 60/106,261, resulting in substantial overlap in the disclosures and claims of those patents.
- There are eleven (11) pending reexaminations ordered by the U.S. Patent Office with respect to those patents, and there is substantial overlap in the art used by the different Examiners to reject the claims.
- Nine of the reexaminations have been pending for over a year, and the other two reexaminations (95/001851 and 95/001856 filed in December 2011) are just a few days short of that mark.
- There is co-pending litigation involving all of the patents in reexamination, including *VirnetX Inc. v. Cisco Systems, Inc.*, No. 6-10-cv-417 (E.D. Tex), and *VirnetX Inc. v. Apple Inc.*, No. 6-12-cv-855 (E.D. Tex.).
- Apple Inc., a third party requestor in proceedings involving the '135 patent, '151 patent, '504 patent, '211 patent, and '181 patent, filed a petition on November 29,

2012, requesting that the Office accelerate the reexamination of Control Nos. 95/001,682, 95/001,949, and 95/001,697.

III. Argument and Action Requested

Cisco hereby respectfully requests that the schedules and handling of the following reexaminations be accelerated, including that future Office Actions set a one-month (or 30 days, whichever is longer) period for response by the Patent Owner:

Reexamination Proceedings To Be Accelerated

Control No.	U.S. Patent	Date Initiated	Examiner
95/001679 & 95/001,682 (merged)	6,502,135	July 8, 2011	Behzad Peikari
95/001714 & 95/001697 (merged)	7,490,151	Aug. 16, 2011	Michael J. Yigdall
95/001746	6,839,759	Sept. 7, 2011	Andrew L. Nalven
95/001792	7,188,180	Oct. 25, 2011	Deandra M. Hughes
95/001851	7,418,504	Dec. 13, 2011	Roland G. Foster
95/001856	7,921,211	Dec. 16, 2011	Roland G. Foster

MPEP 2662(L) provides that in reexaminations such as these, the Office may effectuate its mandate for special dispatch by setting such shortened periods for response:

In addition, if (1) there is litigation concurrent with an inter partes reexamination proceeding and (2) the reexamination proceeding has been pending for more than one year, the Director of the Office of Patent Legal Administration (OPLA), Director of the Central Reexamination Unit (CRU), Director of the Technology Center (TC) in which the reexamination is being conducted, or a Senior Legal Advisor of the OPLA, may approve Office actions in such reexamination proceeding setting a one-month or thirty days, whichever is longer, shortened statutory period for response rather than the two months usually set in reexamination proceedings. A statement at the end of the Office action – “One month or thirty days, whichever is longer, shortened statutory period approved,” followed by the signature of one of these officials, will designate such approval. (MPEP 2662(L).)

All of the patents in reexamination are involved in co-pending litigations, including *VirnetX Inc. v. Cisco Systems, Inc.*, No. 6-10-cv-417 (E.D. Tex), and *VirnetX Inc. v. Apple Inc.*, No. 6-12-cv-855 (E.D. Tex.). Since all of the reexamination proceedings are past or near their filing anniversaries, Cisco asks that a one-month (or 30 day) deadline be set for the Patent Owner’s

response to any Office Action issuing after a proceeding has been pending for more than a year.

Consistent with the need for special dispatch, Cisco also believes that the Patent Office should enforce the shortened period for response by denying any further requests by the Patent Owner to delay the proceeding by extending its deadlines.¹

Apple Inc. filed a Petition under 37 CFR § 1.182 To Align Schedules of Related Proceedings (November 29, 2012). To the extent that the reexamination proceedings are aligned, Cisco believes that no proceeding should be delayed. Rather, Cisco urges that all proceedings be expedited.

As identified in the attached Certificate of Service, a copy of the present petition, in its entirety, is being served to the address of the attorney or agent of record.

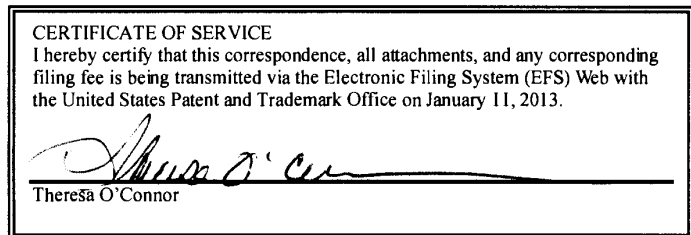
Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: January 11, 2013

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Facsimile: 214/200-0853



¹ Cisco notes that in every reexamination proceeding to date, the Patent Owner has petitioned for, and received, extensions of time allowing it three months to respond to each Office Action. As the Patent Owner is now quite familiar with all of the prior art in these proceedings, such delays are not necessary and should not be accommodated.

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the REVISED PETITION UNDER 37 CFR § 1.182 TO SHORTEN RESPONSE PERIODS AND ACCELERATE PROCEEDINGS was served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

the attorneys of record for the assignee of USP 7,188,180 in accordance with 37 CFR § 1.903, on January 11, 2013.

/David L. McCombs/

David L. McCombs,
Registration No. 32,271

Electronic Acknowledgement Receipt

EFS ID:	14675133
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	11-JAN-2013
Filing Date:	25-OCT-2011
Time Stamp:	12:17:50
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		Revised_Petition_to_Shorten.pdf	185116 8044eb1a313a1747b8d09c9459bcf1517546fc8b	yes	5

Multipart Description/PDF files in .zip description		
Document Description	Start	End
Receipt of Petition in a Reexam	1	4
Reexam Certificate of Service	5	5
Warnings:		
Information:		
Total Files Size (in bytes):		185116
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>		

PATENT

Customer No. 22,852

Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 6,502,135 Edmund Munger et al.))))	Control Nos.: 95/001,679 95/001,682 Examiner: Behzad Peikari
In re U.S. Patent No. 7,490,151 Edmund Munger et al.))))	Control Nos.: 95/001,714 95/001,697 Examiner: Michael J. Yigdall
In re U.S. Patent No. 6,839,759 Victor Larson et al.))))	Control No. 95/001,746 Examiner: Salman Ahmed
In re U.S. Patent No. 7,188,180 Victor Larson et al.))))	Control No.: 95/001,792 Examiner: Deandra M. Hughes
In re U.S. Patent No. 7,418,504 Victor Larson et al.))))	Control No.: 95/001,851 Examiner: Roland G. Foster
In re U.S. Patent No. 7,921,211 Victor Larson et al.))))	Control No.: 95/001,856 Examiner: Roland G. Foster

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 CISCO SYSTEMS, INC.'S PETITION TO SHORTEN
RESPONSE PERIODS AND ACCELERATE PROCEEDINGS**

VirnetX Inc., the owner of the above-referenced patents, opposes third-party requester Cisco Systems, Inc.'s Petition Under 37 CFR § 1.182 to Shorten Response Periods and Accelerate Proceedings ("Petition"). Cisco's dissatisfaction with the progress of the reexaminations is the direct

Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010
Control Nos. 95/001,679; 95/001,682; 95/001,697; 95/001,714; 95/001,746; 95/001,792;
95/001,851; 95/001,856

result of Cisco's own delays and strategic decisions during these proceedings. 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 Nos. 95/001,679 and 95/001,682

Cisco 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 Cisco filed Comments on June 14, 2012. The Office merged this proceeding on December 13, 2012 with a separate reexamination involving the '135 patent. That other reexamination bears control no. 95/001,682 and names Apple Inc. ("Apple") as the real party in interest.

B. Control Nos. 95/001,714 and 95/001,697 ("the '1,697 proceeding")

Cisco filed its Request for Reexamination of U.S. Patent No. 7,490,151 ("the '151 patent") on August 16, 2011. The Office granted the Request and ordered reexamination on October 31, 2011. The Office merged this proceeding on March 15, 2012 with a separate reexamination involving the '151 patent. That other reexamination bears control no. 95/001,697 and names Apple 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 Cisco filed Comments on August 17, 2012.

C. Control No. 95/001,746 (“the ’746 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,839,759 (“the ’759 patent”) on September 7, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on October 14, 2011. Patent Owner timely filed a response to the Office Action on January 17, 2012, and Cisco filed Comments on February 15, 2012.

The Office issued a second Office Action on June 18, 2012. Patent Owner timely filed a response to the second Office Action on August 20, 2012, and Cisco filed Comments on September 18, 2012.

D. Control No. 95/001,792 (“the ’792 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,188,180 (“the ’180 patent”) on October 25, 2011. The Office denied the Request on December 17, 2011. Cisco filed a petition challenging the Office’s denial of the Request on January 17, 2012. The Office granted-in-part Cisco’s petition on September 6, 2012, ordered reexamination, and issued an Office Action on September 19, 2011, which remains pending.

E. Control No. 95/001,851 (“the ’1,851 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,418,504 (“the ’504 patent”) on December 13, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on March 1, 2012. Patent Owner timely filed a response to the Office Action on June 1, 2012, and Cisco filed Comments on June 29, 2012. The Office issued a second Office Action on October 1, 2012, which remains pending.

F. Control No. 95/001,856 (“the ’1,856 proceeding”)

Cisco filed its Request for Reexamination of U.S. Patent No. 7,921, 211 (“the ’211 patent”) on December 16, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on March 5, 2012. Patent Owner timely filed a response to the Office Action on June 5,

2012, and Cisco filed Comments on July 3, 2012. The Office issued a second Office Action on October 1, 2012, which remains pending.

G. Litigation in the Eastern District of Texas

Patent Owner asserted the '135, '759, '180, and '504 patents in a Complaint filed against Cisco 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 '151 and '211 patents in an Amended Complaint filed against Cisco on April 5, 2011. Cisco and its co-defendant, Apple, filed a sealed motion for separate trials on August 31, 2012. The court granted the motion, set Apple's trial date for October 31, 2012, and set Cisco's trial date for March 11, 2013.

Apple and Patent Owner recently concluded their trial. On November 6, 2012, the jury found the asserted claims of the '135, '151, '504, and '211 patents valid and infringed by Apple, awarding Patent Owner over \$368 million in damages. (Ex. A-10.)

II. Argument

As its trial date approaches, Cisco asserts that the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, 95/001,856 proceedings must be accelerated. (Petition 3.) The primary reasons the reexaminations lag so far behind the district-court action, however, are Cisco's own delays and strategic decisions during these proceedings. The Office should not grant the extraordinary relief sought by Cisco for at least these reasons and for the other reasons discussed below.

First, Cisco did not begin to file these reexamination requests until eleven months after the litigation began, and delayed in some instances for up to sixteen months. Cisco has been on notice of Patent Owner's infringement claims based on the '135, '759, '180 and '504 patents at least since Patent Owner filed its first Complaint on August 11, 2010. Yet Cisco did not file requests for reexamination of the '135, '759, '180 and '504 patents until July 8, 2011, September 7, 2011,

Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010
Control Nos. 95/001,679; 95/001,682; 95/001,697; 95/001,714; 95/001,746; 95/001,792;
95/001,851; 95/001,856

October 25, 2011, and December 13, 2011, respectively. Due to Cisco's delays of up to sixteen months in filing, the prosecution of these reexaminations is still before the Central Reexamination Unit. Cisco 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 Cisco. In the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings, Cisco filed enormous requests for reexamination totaling 223, 203, 231, 193, 366, and 366 pages, respectively, including appended claim charts. These requests presented proposed rejections implicating at least 44 different references—several of them well over one hundred pages long. The Office had to review and process all of these papers before issuing Office Actions, and did so within an expeditious timeframe. Cisco could have honed its invalidity positions and filed more targeted reexamination requests to streamline these proceedings, but it did not. Cisco 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 Cisco's vast filings and advancing these reexaminations.

Third, Cisco appears to have been content with the current schedule of the reexaminations throughout their prosecution. Having waited over a year to file many of these reexaminations, Cisco also delayed well beyond the one-year anniversaries of several of these reexamination proceedings before raising any questions regarding the speed of their schedules. (*See id.* at 3.) Cisco's newfound concern, precipitated by its co-defendant Apple's adverse jury verdict and its own now-inconvenient procrastination, does not justify accelerating these proceedings. Doing so would only further burden the Patent Owner and the Office when the Office is already responding with "special dispatch" to the enormous number of issues raised in Cisco's lengthy and late-filed reexamination requests.

Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010
Control Nos. 95/001,679; 95/001,682; 95/001,697; 95/001,714; 95/001,746; 95/001,792;
95/001,851; 95/001,856

Fourth, accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would also substantially prejudice Patent Owner. Along with these proceedings, Patent Owner is concurrently involved in five additional reexaminations naming Apple as the real party in interest, which are also demanding significant attention from Patent Owner. (*See* control nos. 95/001,682; 95/001,788; 95/001,789; and 95/001,949 and the merged proceedings in control nos. 95/001,697 and 95/001,714.) Accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would therefore unreasonably burden Patent Owner and its counsel. Patent Owner would not have sufficient time and opportunity to respond adequately within shortened time periods, given that it must also respond to filings from Apple in a large number of other reexaminations. Indeed, Patent Owner is currently preparing responses to *five* pending Office Actions. (*See* control nos. 95/001,788; 95/001,789; 95/001,792; 95/001,851; and 95/001,856).

Finally, shortening Patent Owner's response periods would not achieve any benefit in these proceedings. Cisco vaguely asserts that "[q]uickly reaching a final decision on the invalidity of the patents in reexamination . . . will ensure that the outcomes of the Office proceedings will be considered in conjunction with related proceedings." (Petition 2.) But if Cisco is referring to the litigation as the "related proceedings," the district court in fact will enter a final judgment and the litigation will reach the Federal Circuit long before the reexaminations will, given the upcoming trial date of March 11, 2013. Thus, even if the Office were to grant Cisco's request (which it should not), the reexaminations will not be ready for appeal to the Federal Circuit for quite some time. Because the relief requested will not help to align the litigation and the reexaminations, and because Cisco is seeking relief from the consequences of its own strategic decisions, shortening Patent Owner's response periods to respond to the enormous number of issues raised in Cisco's lengthy reexamination requests would be unreasonable and prejudicial.

Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010
Control Nos. 95/001,679; 95/001,682; 95/001,697; 95/001,714; 95/001,746; 95/001,792;
95/001,851; 95/001,856

III. Conclusion

The reexaminations are proceeding with the appropriate "special dispatch." Cisco's complaints arise chiefly from its own delay in waiting to file its requests for reexamination, as well as from its own strategic decisions during the course of these reexaminations. Moreover, the relief requested would not promote efficiency, but rather would only prejudice the Patent Owner. Indeed, hurried prosecution of these proceedings would likely result in incomplete consideration of the issues and in fact act to slow the reexaminations. In view of all of the foregoing circumstances, Patent Owner respectfully submits that Cisco's petition should be denied.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 19, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 6,502,135 Edmund Munger et al.)))	Control No.: 95/001,679 95/001,682 Examiner: Behzad Peikari
In re U.S. Patent No. 7,490,151 Edmund Munger et al.)))	Control Nos.: 95/001,714 95/001,697 Examiner: Michael J. Yigdall
In re U.S. Patent No. 6,839,759 Victor Larson et al.)))	Control No. 95/001,746 Examiner: Salman Ahmed
In re U.S. Patent No. 7,188,180 Victor Larson et al.)))	Control No.: 95/001,792 Examiner: Deandra M. Hughes
In re U.S. Patent No. 7,418,504 Victor Larson et al.)))	Control No.: 95/001,851 Examiner: Roland G. Foster
In re U.S. Patent No. 7,921,211 Victor Larson et al.)))	Control No.: 95/001,856 Examiner: Roland G. Foster

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 Cisco Systems, Inc.'s Petition to Shorten Response Periods and Accelerate Proceedings was served by first-class mail on December 19, 2012, on counsel for the third party requesters at the following addresses:

Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010
Control Nos. 95/001,679; 95/001,682; 95/001,697; 95/001,714; 95/001,746; 95/001,792;
95/001,851; 95/001,856

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 19, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14514164
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	19-DEC-2012
Filing Date:	25-OCT-2011
Time Stamp:	15:10:06
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		OpptoCiscospetitiontoaccelerate.pdf	437556 <small>7423eb3158846a3696be50d8eae55404085f9a4</small>	yes	9

Multipart Description/PDF files in .zip description		
Document Description	Start	End
Receipt of Petition in a Reexam	1	7
Reexam Certificate of Service	8	9
Warnings:		
Information:		
Total Files Size (in bytes):		437556
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>		

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor Larson et al.) Control No.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
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:

TRANSMITTAL LETTER

Enclosed please find the following:

1. Patent Owner's Response to Office Action (17 pages);
2. Declaration of Angelos D. Keromytis, Ph.D. (12 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; and
6. Certificate of Service (2 pages).

Please grant any extension of time and charge any additional fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 19, 2012

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.: 95/001,792
)
U.S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
)
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:

PATENT OWNER'S RESPONSE TO
THE OFFICE ACTION OF SEPTEMBER 19, 2012

Table of Contents

I.	Introduction.....	1
II.	Background.....	2
	A. Overview of the '180 Patent	2
	B. Applicable Legal Standards for Anticipation	3
	C. Applicable Legal Standards for Obviousness.....	3
III.	Claims 1, 4, 6-17, 20, 22-33, 35, and 37-41 Are Patentable over the Cited Prior Art.....	4
	A. The Rejection of Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, 39, and 40 Under 35 U.S.C. § 102(b) Based on <i>Kiuchi</i> Should Be Withdrawn.....	4
	1. Overview of <i>Kiuchi</i>	4
	2. Independent Claim 1	5
	3. Independent Claims 17 and 33.....	9
	4. Dependent Claims 6, 22, and 37	9
	5. Dependent Claims 8, 24, and 39	10
	6. Dependent Claims 9, 25, and 40.....	11
	7. Dependent Claims 12 and 28	11
	8. Dependent Claims 13, 15, 29, and 31.....	12
	9. Dependent Claims 16 and 32.....	13
	10. Dependent Claims 4, 10, 14, 20, 26, 30, and 35	13
	B. The Rejection of Claims 11, 27, and 41 Under 35 U.S.C. § 103 Based on <i>Kiuchi</i> Should Be Withdrawn	13
	C. The Rejection of Claims 7, 23, and 38 Under 35 U.S.C. § 103 Based on <i>Kiuchi</i> in View of <i>Martin</i> Should Be Withdrawn.....	14
	D. Secondary Considerations of Nonobviousness.....	15
IV.	Conclusion	17

I. Introduction

VirnetX Inc. (“VirnetX”), the owner of U.S. Patent No. 7,188,180 (“the ’180 patent”), provides the following remarks in response to the Office Action (“OA”) mailed September 19, 2012, and Order granting reexamination (“Order”) mailed September 6, 2012, in the above-identified reexamination proceeding. In the Order, the U.S. Patent and Trademark Office (“USPTO” or “Office”) granted-in-part a petition filed by Cisco Systems, Inc. (“Cisco” or “Requester”) for review of a previous USPTO order denying Cisco’s Request for Reexamination (“Request”), which was filed on October 25, 2011. The Order reaffirmed the Examiner’s determination that there was no “reasonable likelihood” that Requester would prevail on the majority of the proposed rejections, and granted reexamination based on only three of the issues presented by Cisco. (Order at 7-17, *see* “Point 2.”)

The patent at issue in this reexamination (the ’180 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 ’180 patent is a divisional of U.S. application no. 09/558,209 (“the ’209 application”), filed on April 26, 2000 (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent No. 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 No. 7,010,604, “the ’604 patent”), which claims priority to the ’261 and ’704 applications.

The ’180 patent and other patents in this family have been subject to several reexamination proceedings and district court actions. For instance, the ’180 and ’135 patents, along with one other patent from the family, were asserted in an action against Microsoft Corporation (“Microsoft”) in the Eastern District of Texas. The jury found the asserted claims of the ’180 and ’135 patents willfully infringed and not invalid, and awarded VirnetX over \$100 million in damages. (Ex. A-1 at 2.) Microsoft sought reexamination of both the ’180 and ’135 patents, but all claims in both patents were confirmed during those proceedings. (*See* Control Nos. 95/001,269 and 95/001,270.) VirnetX also recently asserted the ’135 patent against Apple Inc. in the Eastern District of Texas, and the jury again found the asserted claims of the ’135 patent infringed and not invalid, awarding VirnetX over \$368 million in damages. (Ex. A-10.)

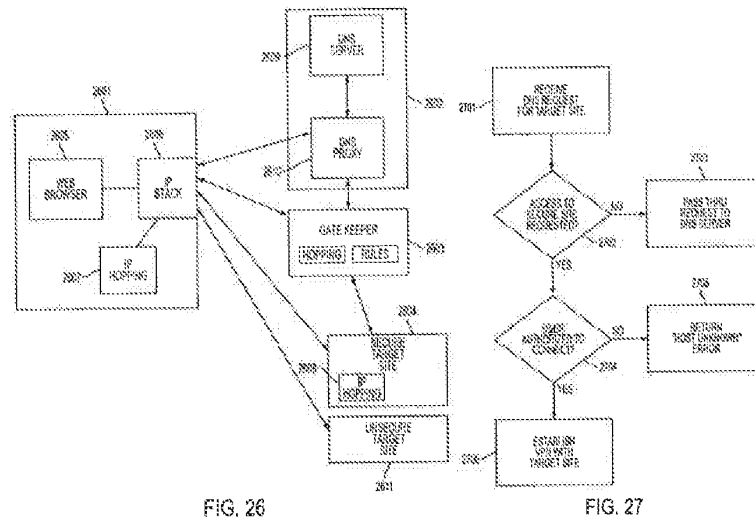
Given that the validity of the ’180 patent and other patents in the Munger patent family has now been tested multiple times, and for other reasons set forth below, including that the asserted references do not disclose or suggest the combination of features recited in the claims, VirnetX requests reconsideration and withdrawal of all the rejections in the Office Action and confirmation of the patentability of all of the claims of the ’180 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, Ph.D. ("Short Decl.").

II. Background

A. Overview of the '180 Patent

The '180 patent discloses several embodiments relating to accessing secure computer network addresses using virtual private network communication links. For example, when a client requests and receives a secure computer network address corresponding to a secure domain name from a secure domain name service, it may send an access request message to the secure computer network address using a virtual private network communication link.



As shown in Figures 26 and 27 of the '180 patent, reproduced above, a client 2601 may receive a secure domain name, such as a secure domain name associated with secure target site 2604. The client 2601 may then send a query message to a specialized, secure DNS server 2602 requesting a secure computer network address corresponding to the secure domain name. ('180 patent 40:36-65.) The client 2601 may receive a response message from the secure DNS server 2602 containing the secure computer network address, and then send an access request message to the secure computer network address using a virtual private network communication link. (*Id.* at 40:46-65.)

The claims of the '180 patent are directed to some of these embodiments. Claims 1, 17, and 33 are independent claims. Claims 2-16 depend directly or indirectly from claim 1, claims 18-32 depend directly or indirectly from claim 17, and claims 34-41 depend directly or indirectly from claim 33. As explained below, none of the references relied upon by the Office Action, 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 Cal.*, 814 F.2d 628, 631 (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, 1371 (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 (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.* § 2143.02(III). Additionally, “[o]bjective evidence relevant to the issue of obviousness must be evaluated by Office personnel.” *Id.* § 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) (emphases added). 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 Burgess*, Appeal No. 2008-2820, 2009 WL 291172 (B.P.A.I. 2009), at *3 (citing *In re Royka*, 490 F.2d 981, 984-85 (C.C.P.A. 1974), and *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970)). A rejection based on obviousness “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.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

III. Claims 1, 4, 6-17, 20, 22-33, 35, and 37-41 Are Patentable over the Cited Prior Art

The Office rejects claims 1, 4, 6-17, 20, 22-33, 35, and 37-41 of the '180 patent as allegedly being anticipated or obvious in view of multiple references. As explained below, however, the references do not disclose or suggest the combination of features recited in the claims.

A. The Rejection of Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, 39, and 40 Under 35 U.S.C. § 102(b) Based on *Kiuchi* Should Be Withdrawn

The Office rejects claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, 39, and 40 under § 102(b) based on Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP — The Development of a Secure, Closed HTTP-based Network on the Internet" (Cisco Req. Ex. D-2) ("*Kiuchi*"). (OA at 2.) For the reasons discussed below, the rejections should be withdrawn and the claims should be confirmed.

1. Overview of *Kiuchi*

Kiuchi proposes a technique called "closed HTTP" ("C-HTTP") for providing secure HTTP communications "within a closed group of institutions on the Internet, where each member is protected by its own firewall." (*Kiuchi* 64.) According to *Kiuchi*, C-HTTP is useful in the medical community, where "there is a strong need for closed networks among hospitals and related institutions" to handle patient data and other sensitive medical information. (*Id.*)

C-HTTP requires three main components: "1) a client-side proxy on the firewall of one institution, 2) a server-side proxy on the firewall of another institution, and 3) a C-HTTP name server, which manages a given C-HTTP-based network and the information for [all of its] proxies." (*Id.*) When an institution wants to participate in a C-HTTP network, it must, among other things, install a client-side and/or server-side proxy on its firewall, register an IP address and a hostname for its proxy, and give the proxy's public key to the C-HTTP name server. (*Id.* at 65.) During C-HTTP communications, "[a] client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol (C-HTTP)." (*Id.* at 64.)

When a user agent computer behind a client-side proxy wants to establish a C-HTTP session with a server behind a server-side proxy, the following C-HTTP setup process occurs:

- (1) The client-side proxy asks the C-HTTP name server whether it can communicate with the server.
- (2) The C-HTTP name server determines whether the server-side proxy is in the closed network and whether the connection is permitted.
- (3) If so, the C-HTTP name server sends the IP address and public key of the server-side proxy, as well as request and response Nonce values, to the client-side proxy.

- (4) The client-side proxy sends a connection request to the server-side proxy, encrypted with the server-side proxy's public key.
- (5) The server-side proxy asks the C-HTTP name server whether the client-side proxy is also in the closed network and whether the connection is permitted.
- (6) If so, the C-HTTP name server sends to the server-side proxy the IP address and public key of the client-side proxy, as well as the same request and response Nonce values previously sent to the client-side proxy.
- (7) The server-side proxy then authenticates the client-side proxy, generates a connection ID, generates a second symmetric key for C-HTTP response encryption, and sends this information to the client-side proxy. When the client-side proxy accepts and checks this information, the connection is established.
- (8) Once the connection is established, a client-side proxy forwards requests from the user agent in encrypted form using C-HTTP format.

(*Id.* at 65-66.) *Kiuchi* explains that “[t]he [C-HTTP] session is finished when the client accesses another C-HTTP server.” (*Id.* at 65.)

2. Independent Claim 1

Claim 1 is directed to a method for accessing a secure computer network address. *Kiuchi* fails to disclose the combination of features recited in this claim for at least the reasons discussed below.

a. *Kiuchi* Fails to Disclose “Sending an Access Request Message . . . Using a Virtual Private Network Communication Link”

Claim 1 recites, among other things, “sending an access request message . . . using a virtual private network communication link.” *Kiuchi* does not disclose this feature for several reasons.

Requester's analysis treats the claim recitations of “sending an access request message” and “using a virtual private network communication link” as separate, unrelated features. (Req. Ex. E-2 at 14-16.) But 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*, 593 F.3d at 1332 (quoting *Lindemann*, 730 F.2d at 1459). Claim 1 in fact specifies that the access request message is sent *using* a virtual private network communication link. Thus, Requester has not properly alleged, much less demonstrated, that *Kiuchi* discloses each and every element of claim 1 as arranged in the claim, and the rejection should therefore be withdrawn. M.P.E.P. § 2131; *Net MoneyIN*, 545 F.3d at 1371.

Specifically, Requester alleges that the “request for connection” in *Kiuchi* corresponds to the “access request message” of claim 1, while a C-HTTP connection between a client-side proxy and a server-side proxy corresponds to the virtual private network communication link. (Req. Ex. E-2 at

14-16.) But *Kiuchi*'s "request for connection" is sent before any C-HTTP connection is established, and accordingly *Kiuchi* fails to disclose "sending an access request message . . . using a virtual private network communication link," as recited in claim 1. (Keromytis Decl. ¶ 22.) Indeed, after a client-side server sends a "request for connection," several subsequent steps must occur before any connection is established between a client-side proxy and a server-side proxy:

- The server-side proxy must ask the name server whether the client-side is an appropriate member of the closed network;
- The name server must examine whether the client-side proxy is permitted to access the server-side proxy;
- The name server must send the IP address and public key of the client-side proxy and the request and response Nonce values to the server-side proxy;
- The server-side proxy must authenticate the client-side proxy and check the integrity of the request;
- The server-side proxy must generate various identification and security-related information;
- The server-side proxy must send that information to the client-side proxy; and
- "When the client-side proxy accepts and checks [the information], the connection is established."

(*Kiuchi* 65-66, describing processes 4 and 5; Keromytis Decl. ¶ 22.) Therefore, a person of ordinary skill would have understood that *Kiuchi*'s request for connection is not sent *using* the alleged virtual private network communication link (the C-HTTP connection), because no C-HTTP connection exists at the time the request for connection is sent. (Keromytis Decl. ¶ 22.)

Kiuchi also does not disclose this claim feature simply because the client-side proxy may send a request for connection using public key encryption. A person of ordinary skill in the art at the time of the invention would not have understood that the mere two steps of contacting a name server to obtain a server-side proxy's public key, and then using that public key to encrypt a request for connection, thereby creates a "virtual private network communication link." (*Id.* ¶ 23; *see Kiuchi* 65, describing processes 2 and 3.) No "link" exists at all between the client-side and server-side proxies at the time the "request for connection" is sent: there is only a one-way communication sent as part of *setting up* the C-HTTP connection. (*Kiuchi* 64-65; Keromytis Decl. ¶ 23.)

Indeed, the public key encryption of a "request for connection" in *Kiuchi* lacks the requisite features of a virtual private network communication link. A person of ordinary skill in the art at the time of the invention would have understood a virtual private network communication link, as recited in claim 1, to be a communication path between computers in a virtual private network. (Keromytis Decl.

¶ 24.) But the “request for connection” in *Kiuchi* is a mere point-to-point communication between two computers that are not yet connected, let alone connected within the same network. (*Kiuchi* 64-65.) In fact, if the client-side proxy is presently engaged in any C-HTTP connection when it attempts to connect to the server-side proxy, *Kiuchi* explains that the connection will be terminated, thus closing any C-HTTP network connection that may have existed. (*Id.* at 65, explaining that a “[C-HTTP] session is finished when the client accesses another C-HTTP server or an ordinary WWW server.”) As a result, when a client-side proxy sends a “request for connection,” the client-side proxy *has no established link to any C-HTTP network or server-side proxy*. (Keromytis Decl. ¶ 24; *Kiuchi* 65.) Rather, the client-side and server-side proxies have simply begun the lengthy process of establishing a connection to each other, and are simply not within any network connection or “virtual private network communication link.” (Keromytis Decl. ¶ 24.)

Moreover, the '180 patent recognizes and distinguishes public key schemes for establishing connections. The '180 patent explains that “[o]ne conventional scheme” involves retrieving the public key of a host from a name server “so that the host can set up a VPN without having the user enter the public key.” ('180 patent 40:6-14.) *Kiuchi* similarly discloses that its client-side proxy retrieves a public key from the C-HTTP name server and uses that public key in sending a “request for connection” to a server-side proxy to eventually set up a C-HTTP connection. (*Kiuchi* 65-66.) Because the '180 patent explicitly recognizes and distinguishes its inventions from conventional public-key-based processes like that disclosed in *Kiuchi* with respect to the “request for connection,” a person of ordinary skill in the art would not have understood *Kiuchi*'s public-key encrypted “request for connection” to disclose a virtual private network communication link, as recited in claim 1. (Keromytis Decl. ¶ 25.)

For at least the above reasons, *Kiuchi* does not disclose “sending an access request message . . . using a virtual private network communication link.” Accordingly, the rejection of claim 1 should be withdrawn, and its patentability confirmed.

b. ***Kiuchi* Fails to Disclose “the Query Message Requesting from the Secure Domain Name Service a Secure Computer Network Address Corresponding to the Secure Domain Name”**

Independent claim 1 also recites “the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name.” The Office contends that *Kiuchi* discloses this feature because “[a] client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL” and “the C-HTTP name server sends the IP address . . . of the server-side proxy.” (*See* Req. Ex. E-2 at 10-11, quoting *Kiuchi* 65.) According to the Office, the URL is the claimed “secure domain name” while the IP address of the

server-side proxy is the claimed "secure computer network address" corresponding to it. This is incorrect.

As Patent Owner's expert successfully demonstrated to the court at trial in the *VirnetX v. Apple* litigation, *Kiuchi*'s URL (the alleged secure domain name) does not correspond to the *server-side proxy*, but rather to the *resource itself* located on an origin server. (See 11/05/2012 Trial Tr. Afternoon Sess. 39:3-41:20, attached as Ex. A-11.) For example, *Kiuchi* explains that the URL "http://server.in.current.connection/sample.html=@=6zdDfldfcZLj8Vli" represents a "resource name," and when the URL is clicked, "the client-side proxy takes off the connection ID and forwards, the stripped, the original *resource name* to the *server* . . ." (*Kiuchi* 65, emphases added.) As a result, the URL (the alleged secure domain name) does not correspond to the IP address of the *server-side proxy* (the alleged secure computer network address) but to a *resource on the origin server*. And when the C-HTTP name server is provided with the URL of a resource, it responds not with the resource's corresponding address but with the IP address of the server-side proxy. Accordingly, the name service request in *Kiuchi* does not request "a secure computer network address corresponding to the secure domain name," as recited in claim 1.

Patent Owner notes that Appendix 2.1 of *Kiuchi* describes the format of a "C-HTTP name service request." (*Id.* at 72.) As shown, the name service request includes a field "SERVER-SIDE-PROXY-NAME." (*Id.*) However, as Patent Owner's expert explained at trial, one of ordinary skill in the art would have recognized that this field in fact refers to the URL of the *resource* on the origin server being requested, not to the domain name of the *server-side proxy*. (Ex. A-11 at 39:20-40:11.) In fact, Dr. Kiuchi confirmed that this is the case in a 1996 slide presentation on C-HTTP accompanying his paper that he gave to the Institute of Electrical and Electronics Engineers ("IEEE"). (See generally *Kiuchi* Slide Presentation, attached as Ex. A-12.) For example, slide 9 explains that the C-HTTP name server "keeps" "resource names." (*Id.* at 9.) Additionally, slide 17 illustrates that a C-HTTP name request includes a "RESOURCE-NAME" (*id.* at 17), while slide 20 shows that the C-HTTP name response that follows includes a "SERVER-SIDE-PROXY-IP [address]" (*id.* at 20). Indeed, *Kiuchi*'s system would not work if the client-side proxy provided to the C-HTTP name server a domain name of the server-side proxy rather than a resource name corresponding to a desired resource on an origin server. (See Ex. A-11 at 40:15-20, "Q. Would the *Kiuchi* system work if the client-side proxy requested a domain name for the server-side proxy from C-HTTP? A. No. The way *Kiuchi* has to work is that what's being requested is the resource that's on the origin server. That's where the data is.") As a result, *Kiuchi* does not enable any embodiment in which the client-side proxy requests from the secure domain name service a secure computer network address corresponding to a secure domain name.

3. Independent Claims 17 and 33

Independent claims 17 and 33 include recitations similar to those described above regarding claim 1. For example, like claim 1, claims 17 and 33 also recite “a secure computer network address” and “sending an access request message . . . using a virtual private network communication link.” *Kiuchi* does not disclose these features of claims 17 and 33 for at least the reasons discussed above with respect to claim 1. Accordingly, Patent Owner requests that the rejection of claims 17 and 33 be withdrawn, and their patentability confirmed.

4. Dependent Claims 6, 22, and 37

Dependent claims 6, 22, and 37 depend from independent claims 1, 17, and 33, respectively, and include all of their features. In addition to the reasons set forth above regarding claims 1, 17, and 33, *Kiuchi* does not anticipate claims 6, 22, and 37 because *Kiuchi* does not disclose that “the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.”

Requester admits that *Kiuchi* does not explicitly disclose these additional claim features by arguing that a separate reference, RFC 793, indicates that TCP connections employ “type of service” fields. But anticipation rejections cannot rely on multiple references, except in limited circumstances, such as to show that a characteristic not disclosed in a reference is otherwise inherent. M.P.E.P. § 2131.01; *see also Verdegaal*, 814 F.2d at 631 (“A claim is anticipated only if each and every element as set forth in the claim is found . . . in a single prior art reference.”). Here, Requester has neither shown nor attempted to show that *Kiuchi*’s C-HTTP system would *necessarily* “insert[] into at least one data packet at least one data value representing a predetermined level of service,” as recited in the claims. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Thus, the rejection of claims 6, 22, and 37 is improper and should be withdrawn.

Moreover, *Kiuchi* does not disclose, and Requester does not identify, any nexus between RFC 793’s “type of service” fields and the alleged virtual private network (i.e., the C-HTTP connection) or a predetermined level of service associated with a C-HTTP connection. Thus, *Kiuchi* does not disclose that its C-HTTP connection is “based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network,” as recited in claims 6, 22, and 37 (emphasis added). (Keromytis Decl. ¶ 27.) Instead of addressing the precise arrangement of features in this claim language, Requester sidesteps the issue by vaguely asserting that “it is understood” that *Kiuchi*’s various transactions merely *use* a data value representing a predetermined level of service. (Req. Ex. E-2 at 22.) This fails to show that *Kiuchi* expressly or inherently discloses each and every element of claims 6, 22, and 37. *Verdegaal*, 814 F.2d at 631. The rejections should be

withdrawn.

5. Dependent Claims 8, 24, and 39

Dependent claims 8, 24, and 39 depend from independent claims 1, 17, and 33, respectively, and include all of their features. In addition to the reasons set forth above regarding claims 1, 17, and 33, *Kiuchi* does not anticipate claims 8, 24, and 39 because *Kiuchi* does not disclose that “the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.”

Requester alleges that the Nonce values contained in the headers of *Kiuchi*’s C-HTTP requests and responses constitute the claimed “value in each data packet.” (Req. Ex. E-2 at 22-24.) Specifically, Requester alleges that, “[i]n the Examples of C-HTTP communication found in Appendix 3, it can be seen that the ‘Request-Nonce value’ is incremented, moving from ‘8abd853f’ in Example c., to ‘8abd8540’ in Example g., to ‘8abd8541’ in Example i.” (*Id.* at 23.) According to *Kiuchi*, Example c. is a “Request for connection to the server-side proxy,” Example g. is “Sending C-HTTP requests to the server-side proxy,” and Example i. is a “Request for closing the connection.” (*Kiuchi* 74.) This shows that different types of requests might contain different Nonce values, but the Requester has not shown, and *Kiuchi* does not disclose, that these Nonce values are compared to “a moving window of valid values,” as recited in claim 12. (See Keromytis Decl. ¶ 29.) *Kiuchi* just mentions that the “[r]eplay attacks are blocked by *checking* values of the Request-Nonce header field.” (*Kiuchi* at 65, emphasis added.) *Kiuchi* does not explain *how* the values of the Nonce header field are checked, and certainly does not teach that they are checked by comparing them to a moving window of valid values. Furthermore, there are many ways that the values of the Nonce header field could be checked without comparing them to a moving window of valid values. (Keromytis Decl. ¶ 29.) Thus, this feature is neither disclosed by, nor inherent in, *Kiuchi*.

In addition, as discussed, *Kiuchi* teaches that C-HTTP *requests* and *responses* may contain a Nonce value in a Nonce header field. (See *Kiuchi* 65, 71.) But *Kiuchi* does not teach that such Nonce values are inserted into *each data packet*. (Keromytis Decl. ¶ 30.) Accordingly, even if the Nonce values were compared to a moving window of valid values (which they are not), *Kiuchi* still does not disclose that the virtual private network is based on comparing a value in *each data packet* transmitted between the first computer and the second computer to a moving window of valid values, as claimed. One of ordinary skill in the art would not have considered *Kiuchi*’s C-HTTP requests and responses, which are application layer requests, to be data packets. (*Id.*) Thus, the rejection of claims 8, 24, and 39 is improper and should be withdrawn.

6. Dependent Claims 9, 25, and 40

Dependent claims 9, 25, and 40 depend from independent claims 1, 17, and 33, respectively, and include all of their features. In addition to the reasons set forth above regarding claims 1, 17, and 33, *Kiuchi* does not anticipate claims 9, 25, and 40 because *Kiuchi* does not disclose that “the virtual private network is based on a comparison of a discriminator field in a header of *each data packet* to the secure computer network address to a table of valid discriminator fields” (emphasis added).

Requester asserts that a connection ID in *Kiuchi* corresponds to a “discriminator field,” and that two different *Kiuchi* passages each disclose the “comparison of a discriminator field in a header of each data packet . . . to a table of valid discriminator fields.” (Req. Ex. E-2 at 26.) This is incorrect.

First, Requester argues that *Kiuchi* discloses these claim features because a C-HTTP connection will be disconnected if a connection ID contained in a resource name is not found in a current connection table. (*Id.*) Specifically, *Kiuchi* explains that “[w]hen one of these resource names with a connection ID . . . is selected and requested by an end-user, the client-side proxy takes off the connection ID When the connection ID is not found in the current connection table in the client-side-proxy, the current connection is disconnected.” (*Kiuchi* 65.) But claims 9, 25, and 40 recite a discriminator field “in a header of *each data packet*” (emphasis added), not a discriminator field constituting a portion of a resource name. Thus, the first feature of *Kiuchi* asserted by Requester fails to disclose the recited “comparison.”

Second, Requester argues that the recited comparison is disclosed because *Kiuchi* explains that “if the server-side proxy detects that a given connection times out, it deletes the connection ID from the connection list, informing the client-side proxy that the connection is closed when an error status is returned in response to the request.” (Req. Ex. E-2 at 26, quoting *Kiuchi* 67.) But nowhere does *Kiuchi* teach that a connection ID is contained in *each data packet*, or that the virtual private network is based on a comparison of a discriminator field in a header of each data packet, as recited in the claims. Rather, Requester’s asserted passage indicates that the C-HTTP connection is, if anything, “based on” a timer, not on a connection ID. (Keromytis Decl. ¶ 33.) Indeed, the connection ID will endure beyond the termination of a C-HTTP connection until the server-side proxy eventually detects that the connection has already timed out. (*Id.*; *Kiuchi* 67.)

Accordingly, *Kiuchi* fails to disclose the features of claims 9, 25, and 40, and the rejection should be withdrawn.

7. Dependent Claims 12 and 28

Dependent claims 12 and 28 depend from independent claims 1 and 17, respectively, and include all of their features. In addition to the reasons set forth above regarding claims 1 and 17, *Kiuchi* does not

anticipate claims 12 and 28 because *Kiuchi* does not disclose that “the access request message contains a request for information stored at the secure computer network address.”

Requester asserts that *Kiuchi* discloses “a request for information stored at the secure computer network address” because a server-side proxy may provide a connection ID and a second symmetric data exchange key to the client-side proxy. (Req. Ex. E-2 at 28.) But *Kiuchi* discloses that the connection ID and second symmetric data exchange key are not *stored* at the secure computer network address, as recited in the claims, but rather are *newly generated* after the server-side proxy receives information regarding the client-side proxy from the C-HTTP name server. (*Kiuchi* 66; Keromytis Decl. ¶ 35.) Indeed, “[w]hen the server-side proxy obtains the client-side proxy’s [information], it . . . generates both a connection ID . . . and also a second symmetric data exchange key for response encryption, which are sent to the client-side proxy.” (*Kiuchi* 66.) Thus, the “request for connection” in *Kiuchi* alleged to correspond to the “access request message” cannot contain a request for information stored at the server-side proxy, because that information, yet to be generated, is not stored at the server-side proxy at the time the message is sent. (Keromytis Decl. ¶ 35.)

Thus, *Kiuchi* fails to disclose the features of claims 12 and 28, and the rejection should be withdrawn.

8. Dependent Claims 13, 15, 29, and 31

Dependent claims 13 and 29 depend from independent claims 1 and 17, respectively, and include all of their features. In addition to the reasons discussed above regarding claims 1 and 17, *Kiuchi* does not anticipate claims 13 and 29 because *Kiuchi* does not disclose the various features of claims 1 and 17 occurring “at the client computer.” Claims 15 and 31, also depending from claims 1 and 17, respectively, similarly recite “[t]he method . . . performed by a client computer.” *Kiuchi* does not disclose these features.

Requester asserts that in *Kiuchi*, “[t]he client-side proxy is the client computer as claimed.” (Req. Ex. E-2 at 29-30.) But this is incorrect: *Kiuchi* clearly distinguishes between clients and client-side proxies. (*Kiuchi* 64.) *Kiuchi* describes “user agents” as entities *within a firewall*, while explaining that the client-side proxy resides *on the firewall* of an institution, for example, a hospital. (*Id.*, explaining that the C-HTTP system *requires* “a client-side proxy on the firewall of one institution” and a server-side proxy on the firewall of another institution.)

In fact, one of the motivations for designing the C-HTTP system involving mandatory client-side and server-side proxies was the problem that “[i]t is not realistic for hospital information managers to expect that all *individual end-users*, including those who connect their PCs to in-hospital LANs, manage their keys in a secure manner.” (*Id.* at 68, emphasis added.) A person of ordinary skill at the time of the

invention would have been readily capable of distinguishing, as *Kiuchi* does, between client computers within an institutional firewall (e.g., a nurse's or doctor's PC in a hospital) and a computer residing on an institutional firewall (e.g., a client-side proxy). (Keromytis Decl. ¶ 38.) By asserting the equivalence of *Kiuchi*'s client-side proxy to a "client computer," Requester ignores the plain language of the claims and distorts the teachings of *Kiuchi*.

Accordingly, *Kiuchi* does not disclose the features of claims 13, 15, 29, and 31, and the rejection should be withdrawn.

9. Dependent Claims 16 and 32

Dependent claims 16 and 32 depend from claims 2 and 18, and include all of their features. Because the Office did not adopt Requester's proposed rejections of claims 2 and 18 due to *Kiuchi*'s failure to teach the elements of claims 2 and 18, Patent Owner respectfully submits that the rejection of claims 16 and 32 is improper and should be withdrawn. (See Order at 10-11.)

10. Dependent Claims 4, 10, 14, 20, 26, 30, and 35

Dependent claims 4, 10, 14, 20, 26, 30, and 35 depend from one of independent claims 1, 17, or 33, and include all of their features. Accordingly, *Kiuchi* does not anticipate any of these claims for at least the reasons discussed above in conjunction with claims 1, 17, and 33. Thus, the rejections of these claims should be withdrawn, and their patentability confirmed.

B. The Rejection of Claims 11, 27, and 41 Under 35 U.S.C. § 103 Based on *Kiuchi* Should Be Withdrawn

Dependent claims 11, 27, and 41 depend from independent claims 1, 17, and 33, respectively, and include all of their features. In addition to the reasons discussed above regarding claims 1, 17, and 33, *Kiuchi* does not disclose or suggest any of the features of claims 11, 27, and 41 because *Kiuchi* does not disclose or suggest that "the secure domain name has a top-level domain name that includes one of .com, .net, .org, .edu, .mil or .gov."

The Office and Requester assert that it would have been obvious, as a design choice, to use a top-level domain name that includes one of .com, .net, .org, .edu, .mil, or .gov. (OA at 3; Req. Ex. E-2 at 51-52.) But neither the Office nor Requester have provided anything remotely resembling the "articulated reasoning" required to support an obviousness rejection. *KSR*, 550 U.S. at 418. Requester makes the conclusory assertion that the additional features of claims 11, 27, and 41 "merely arrange[] known elements in a configuration recognized as functionally equivalent to a known configuration," but provides no evidence whatsoever to suggest that adding letters to conventional top-level domain names was known in or suggested by the art at the time of the invention. (Req. Ex. E-2 at 51, quoting *Ex parte Gunasekar* at 9, Appeal No. 2009-008345, in 10/903,590 (B.P.A.I. 2011).) Indeed, just like in *Gunasekar*, Requester "has not provided any persuasive evidence that the [claim feature] as recited in

[the] claim was a known alternative.” *Gunasekar* at 10.

Far from suggesting succinct alterations to top-level domain names, *Kiuchi* discloses making lengthy alterations and appending unwieldy character strings to domain names for use in its C-HTTP system. For example, *Kiuchi* employs the *nonconventional* “.CSCRG” to denote that a name is a C-HTTP name, which does not disclose or suggest modifying a conventional top-level domain name, much less modifying such a domain name to indicate security features. (*Kiuchi* 73.) Nor can *Kiuchi* make any such suggestion, as *Kiuchi* does not discuss its .CSCRG names at all. Instead, it merely lists them in an appendix of example C-HTTP communications without explanation. (*Id.*) As an additional example, *Kiuchi* discloses that its system will simply append connection IDs to resource names, for example, “http://server.in.current.connection/sample.html@@=6zdDfldfcZLj8Vlj,” which also does not suggest succinctly modifying a top-level domain name. (*Id.* at 65, emphasis added.) These burdensome naming features may make sense in *Kiuchi*, where clients are quite insulated from the mechanisms of the C-HTTP system by proxies. (*See supra* section III.B.8, explaining that *Kiuchi* does not disclose the features of independent claims 1, 17, and 33 “performed by a client computer.”) But claims 11, 27, and 41 are not as specifically limited as *Kiuchi* in this manner. Nothing in *Kiuchi*’s limited disclosures would disclose or suggest succinctly modifying a top-level domain name to denote security; rather, *Kiuchi*’s lengthy and unwieldy domain names suggest the exact opposite.

Accordingly, *Kiuchi* does not disclose or suggest the features of claims 11, 27, and 41, and the rejections of those claims should be withdrawn, as they cannot be supported by Requester’s conclusory and unsupported assertions.

C. The Rejection of Claims 7, 23, and 38 Under 35 U.S.C. § 103 Based on *Kiuchi* in View of *Martin* Should Be Withdrawn

Dependent claims 7, 23, and 38 depend indirectly from independent claims 1, 17, and 33, respectively, and include all of their features. In addition to the reasons discussed above regarding claims 1, 17, and 33, *Kiuchi* in view of *Martin*, D.M., “A Framework for Local Anonymity in the Internet” (“*Martin*”), does not disclose or suggest any of the features of claims 7, 23, and 38 because these references do not disclose or suggest that the “virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.”

Kiuchi does not disclose “a computer network address hopping regime that is used to pseudorandomly change computer network addresses.” Nor does Requester assert that it does. Instead, Requester relies on *Martin* to allegedly show these claim features. (Req. Ex. E-2 at 47-48.) But *Martin* does not disclose these features, as illustrated by Requester’s tangential assertion that *Martin* describes “[c]hoosing one of the source addresses ‘at random.’” (*Id.* at 48.) This is not what the claims recite.

Claims 7, 23, and 38 recite that “the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets.” *Martin* does not disclose pseudorandomly changing network addresses in packets, let alone a network address hopping regime that is used to pseudorandomly change network addresses in packets. (*See Martin* 9.) Because Requester fails to even assert that *Martin* discloses these features or explain how the combination of *Kiuchi* and *Martin* would render these missing features obvious, the rejection is improper on its face and should be withdrawn, and the patentability of claims 7, 23, and 38 should be confirmed.

Accordingly, Patent Owner respectfully requests that the rejection of claims 1, 4, 6-17, 20, 22-33, 35, and 37-41 under 35 U.S.C. §§ 102(b) and 103 be withdrawn, and that their patentability be confirmed.

D. Secondary Considerations of Nonobviousness

“Objective evidence relevant to the issue of obviousness *must* 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, Inc.*, 679 F.3d 1372, 1378 (Fed. Cir. 2012) (citation 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 not.” *Id.* (emphasis added) (citations omitted). Objective indicia include 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.

The claimed inventions have 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 '180 patent on July 2002. (Short Decl. ¶ 12.) Microsoft, Aastra, Mitel, and NEC have all since entered into patent licensing agreements with VirnetX that include the '180 patent. (*Id.*) In addition, Microsoft was found to willfully infringe the '180 patent and one other patent in the Munger patent family, leading to a damages award of over \$100 million. (*Id.*; Ex. A-1 at 2.)

By providing systems and methods for easily enabling secure communications, the inventions of the '180 patent have satisfied a long-felt need and succeeded where others failed. (Short Decl. ¶ 11.) Prior to the effective filing date of the '180 patent, there was a significant concern for security in computer network communications. (*Id.* ¶ 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.* ¶¶ 8, 11.) Specifically, remote access was “a nightmare” for support desks, and adding the commercially available VPN software was even more difficult. (*Id.* ¶ 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.* ¶ 9.)

Many organizations tried and failed to provide a solution that allowed a user to easily and conveniently enable secure communications. (*Id.* ¶ 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.* ¶ 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 '180 patent and its patent family. (*Id.* ¶ 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 '180 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 '180 patent. (*Id.* ¶ 7.) The year the inventions claimed in the '180 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.* ¶ 14.) For example, a program manager for DARPA informed Edmund Munger, a coinventor of the '180 patent, that the technology would never be adopted. (*Id.* ¶ 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 '180 patent was adopted, and even received praise by those in the field. (*Id.* ¶ 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.* ¶ 7.) Meanwhile, as discussed

above, SafeNet, Microsoft, Aastra, Mitel, and NEC have all obtained licenses from VirnetX to practice the inventions disclosed in the '180 patent.

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, 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 '180 patent.

VirnetX notes that the Request, Order, and Office Action contain a number of assertions and allegations concerning the '180 patent disclosure, '180 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 and charge any required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 19, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexaminations of:)
Victor Larson et al.) Control No.: 95/001,792
U.S. Patent No. 7,188,180) Group Art Unit: 3992
Issued: March 6, 2007) Examiner: Deandra M. Hughes
For: METHOD FOR ESTABLISHING SECURE) Confirmation Nos. 1972
COMMUNICATION LINK BETWEEN)
COMPUTERS OF VIRTUAL PRIVATE)
NETWORK)

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. 7,188,180 ("the '180 patent"). I further understand that the '180 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 '180 patent is a divisional of U.S. application no. 09/558,209 ("the '209 application") filed April 26, 2000, which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent 6,502,135, "the '135 patent"), and that the '135 patent is a continuation-in-part of U.S. application no. 09/429,643 (now U.S. Patent No. 7,010,604, "the '604 patent"), which claims priority to the '261 and '704 applications.

I. RESOURCES I HAVE CONSULTED

2. I have reviewed the '180 patent, including claims 1-41. I have also reviewed a Request for *Inter Partes* Reexamination of the '180 patent filed by Cisco Systems, Inc. with the U.S. Patent and Trademark Office ("Office") on October 25, 2011 ("Request" or "Req."), as well as the

exhibits accompanying the Request. Additionally, I have reviewed an order granting reexamination of the '180 patent ("the Order") mailed on September 6, 2012, and an Office Action ("the Office Action") mailed on September 19, 2012.¹

3. I have also studied the following documents cited in and included with the Request and Office Action: Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP — The Development of a Secure, Closed HTTP-based Network on the Internet" ("*Kiuchi*"); and D.M. Martin "A Framework for Local Anonymity in the Internet" ("*Martin*").

4. I am familiar with the level of ordinary skill in the art with respect to the inventions of the '180 patent as of February 15, 2000, when the application for the '135 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.

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

¹ The Office Action incorporates certain portions of the Request by reference. For that reason, when I sometimes refer to "the Request," I am also referring to the Office Action.

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 thirty-six 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.

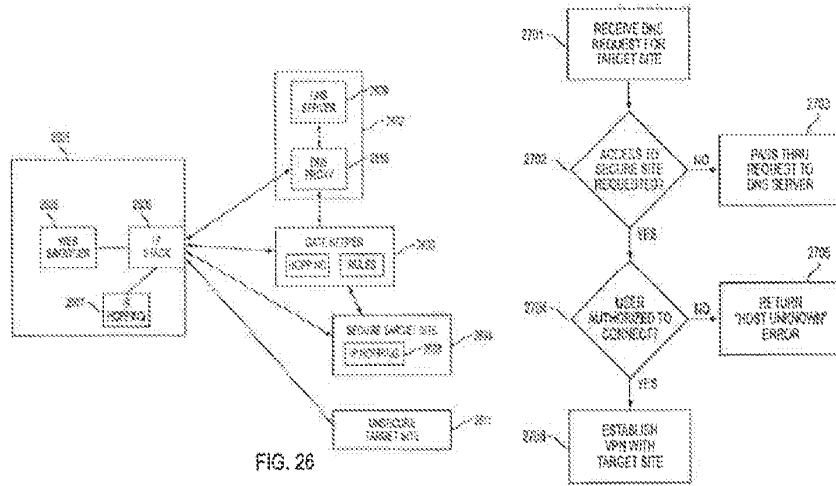
12. I have chaired several international technical conferences and workshops in cybersecurity, including, for example, the International Conference on Financial Cryptography and Data Security (“FC”), ACM Computer and Communication Security (“CCS”), and the New Security Paradigms Workshop (“NSPW”). I 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 malicious cyber-insider threats, 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 '180 PATENT

15. Before turning to a discussion of the references relied on in the Request and the Office Action, I summarize my understanding of certain embodiments disclosed in the '180 patent. Generally speaking, the '180 patent discloses several embodiments relating to accessing secure computer network addresses using virtual private network communication links. For example, when a client requests and receives a secure computer network address corresponding to a secure domain name from a secure domain name service, it may send an access request message to the secure computer network address using a virtual private network communication link.



16. As shown in Figures 26 and 27 of the '180 patent, reproduced above, a client 2601 may receive a secure domain name, such as a secure domain name associated with secure target site 2604. The client 2601 may then send a query message to a specialized, secure DNS server 2602 requesting a secure computer network address corresponding to the secure domain name. ('180 patent 40:36-65.) The client 2601 may receive a response message from the secure DNS server 2602 containing the secure computer network address, and then send an access request message to the secure computer network address using a virtual private network communication link. (*Id.* at 40:46-65.)

17. I understand the claims of the '180 patent to be directed to some of these embodiments.

IV. KIUCHI

18. Generally, *Kiuchi* proposes a technique called “closed HTTP” (C-HTTP) for providing secure HTTP communications “within a closed group of institutions on the Internet, where each member is protected by its own firewall.” (*Kiuchi* 64.) According to *Kiuchi*, C-HTTP is useful in the medical community, where “there is a strong need for closed networks among hospitals and related institutions” to handle patient data and other sensitive medical information. (*Id.*)

19. C-HTTP requires three main components: “1) a client-side proxy on the firewall of one institution, 2) a server-side proxy on the firewall of another institution, and 3) a C-HTTP name server, which manages a given C-HTTP-based network and the information for [all of its] proxies.” (*Id.*) When an institution wants to participate in a C-HTTP network, it must, among other things, install a client-side and/or server-side proxy on its firewall, register an IP address and a hostname for its proxy, and give the proxy’s public key to the C-HTTP name server. (*Id.* at 65.) During C-HTTP communications, “[a] client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol (C-HTTP).” (*Id.* at 64.)

20. When a user agent computer behind a client-side proxy wants to establish a C-HTTP session with a server behind a server-side proxy, the following C-HTTP setup process occurs:

- (1) The client-side proxy asks the C-HTTP name server whether it can communicate with the server.
- (2) The C-HTTP name server determines whether the server-side proxy is in the closed network and whether the connection is permitted.
- (3) If so, the C-HTTP name server sends the IP address and public key of the server-side proxy, as well as request and response Nonce values, to the client-side proxy.
- (4) The client-side proxy sends a connection request to the server-side proxy, encrypted with the server-side proxy’s public key.
- (5) The server-side proxy asks the C-HTTP name server whether the client-side proxy is also in the closed network and whether the connection is permitted.
- (6) If so, the C-HTTP name server sends to the server-side proxy the IP address and public key of the client-side proxy, as well as the same request and response Nonce values previously sent to the client-side proxy.
- (7) The server-side proxy then authenticates the client-side proxy, generates a connection ID, generates a second symmetric key for C-HTTP response encryption, and sends this information to the client-side proxy. When the

client-side proxy accepts and checks this information, the connection is established.

(8) Once the connection is established, a client-side proxy forwards requests from the user agent in encrypted form using C-HTTP format.

(*Id.* at 65-66.) *Kiuchi* explains that “[t]he [C-HTTP] session is finished when the client accesses another C-HTTP server.” (*Id.* at 65.)

A. Independent Claims 1, 17, and 33

21. I understand that claim 1 recites “sending an access request message . . . using a virtual private network communication link.” I also understand that the Request alleges that the “request for connection” in *Kiuchi* corresponds to the “access request message” of claim 1, and that a C-HTTP connection between a client-side proxy and a server-side proxy corresponds to the virtual private network communication link. (Req. Ex. E-2 at 14-16.) I disagree.

22. *Kiuchi*’s “request for connection” is sent before any C-HTTP connection is established, and accordingly it cannot correspond to “sending an access request message . . . using a virtual private network communication link.” In fact, after a client-side server sends a “request for connection” in *Kiuchi*, several subsequent steps must occur before any connection is established between a client-side proxy and a server-side proxy:

- The server-side proxy must ask the name server whether the client-side is an appropriate member of the closed network;
- The name server must examine whether the client-side proxy is permitted to access the server-side proxy;
- The name server must send the IP address and public key of the client-side proxy and the request and response Nonce values to the server-side proxy;
- The server-side proxy must authenticate the client-side proxy and check the integrity of the request;
- The server-side proxy must generate various identification and security-related information;
- The server-side proxy must send that information to the client-side proxy; and
- “When the client-side proxy accepts and checks [the information], the connection is established.”

(*Kiuchi* 65-66, describing processes 4 and 5.) Therefore, a person of ordinary skill would have understood that *Kiuchi*’s request for connection is not sent *using* the alleged virtual private network

communication link (the C-HTTP connection), because no C-HTTP connection exists at the time the request for connection is sent.

23. A person of ordinary skill in the art at the time of the invention would also have understood that the mere two steps of (1) contacting a name server to obtain a server-side proxy's public key, and then (2) using that public key to encrypt a request for connection, do not thereby create a "virtual private network communication link." This is because, in this situation, no "link" exists at all between the client-side and server-side proxies at the time the "request for connection" is sent. Rather, there is only a one-way communication sent as part of *setting up* the C-HTTP connection. (*Kiuchi* 64-65.)

24. Moreover, the public key encryption of a "request for connection" in *Kiuchi* lacks the requisite features of a virtual private network communication link. A person of ordinary skill in the art would have understood a virtual private network communication link, as recited in claim 1, to be a communication path between computers in a virtual private network. The "request for connection" in *Kiuchi*, by comparison, is a mere point-to-point communication between two computers that are not yet connected, let alone connected within the same network. (*Kiuchi* 64-65.) In fact, if the client-side proxy is presently engaged in any C-HTTP connection when it attempts to connect to the server-side proxy, *Kiuchi* explains that the connection will be terminated, thus closing any C-HTTP network connection that may have existed. (*Kiuchi* 65, explaining that a "[C-HTTP] session is finished when the client accesses another C-HTTP server or an ordinary WWW server.") As a result, when a client-side proxy sends a "request for connection," the client-side proxy has no link to any C-HTTP network or server-side proxy. (*Kiuchi* 65.) Rather, the client-side and server-side proxies have simply begun the lengthy process of establishing a connection to each other, and are simply not within any network connection or "virtual private network communication link."

25. The '180 patent also explicitly recognizes and distinguishes public key schemes for establishing connections, like the *Kiuchi* public key encryption discussed above. The '180 patent explains that "[o]ne conventional scheme" involves retrieving the public key of a host from a name server so that the host can set up a VPN without having the user enter the public key." ('180 patent 40:6-14.) *Kiuchi* similarly discloses that its client-side proxy retrieves a public key from the C-HTTP name server and uses that public key in sending a "request for connection" to a server-side proxy to eventually set up a C-HTTP connection. (*Kiuchi* 65-66.) Accordingly, a person of ordinary skill in the art would not have understood *Kiuchi*'s public-key encrypted "request for connection" to correspond to the virtual private network communication link recited in claim 1.

B. Claims 6, 22, and 37

26. I understand that claims 6, 22, and 37 recite that “the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.” I also understand that the Request, citing to RFC 793, asserts that TCP connections employ “type of service” fields which correspond to “inserting into at least one data packet at least one data value representing a predetermined level of service.” I disagree.

27. *Kiuchi* simply does not describe any nexus between RFC 793’s “type of service” fields and the alleged virtual private network (i.e., the C-HTTP connection) or a predetermined level of service associated with a C-HTTP connection. Thus, a person of ordinary skill would not have understood *Kiuchi*’s C-HTTP connection to be “based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.” Accordingly, a person of ordinary skill would not have understood *Kiuchi* to show, either expressly or inherently, that “the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network,” as recited in claims 6, 22, and 37.

C. Claims 8, 24, and 39

28. I understand that claims 8, 24, and 39 recite that “the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.” I also understand that the Request alleges that the Nonce values contained in the headers of *Kiuchi*’s C-HTTP requests and responses correspond to the “value in each data packet” recited in claims 8, 24, and 39. (Req. Ex. E-2 at 22-24.) I disagree.

29. The Request alleges that, “[i]n the Examples of C-HTTP communication found in Appendix 3, it can be seen that the ‘Request-Nonce value’ is incremented, moving from ‘8abd853f’ in Example c., to ‘8abd8540’ in Example g., to ‘8abd8541’ in Example i.” (*Id.* at 23.) According to *Kiuchi*, Example c. is a “Request for connection to the server-side proxy,” Example g. is “Sending C-HTTP requests to the server-side proxy,” and Example i. is a “Request for closing the connection.” (*Kiuchi* 74.) Although this shows that different types of requests might contain different Nonce values, *Kiuchi* does not disclose that these Nonce values are compared to “a moving window of valid

values,” as recited in claim 12.² *Kiuchi* just mentions that the “[r]eplay attacks are blocked by checking values of the Request-Nonce header field.” (*Id.* at 65, emphasis added.) *Kiuchi* does not explain *how* the values of the Nonce header field are checked, and certainly does not teach that they are checked by comparing them to a moving window of valid values. In fact, there are many ways that the values of the Nonce header field could be checked without comparing them to a moving window of valid values. Thus, this feature is neither taught in, nor inherent in, *Kiuchi*.

30. Furthermore, *Kiuchi* teaches that C-HTTP requests and responses may contain a Nonce value in a Nonce header field. (See *Kiuchi* 65, 71.) But *Kiuchi* does not teach that such Nonce values are inserted into *each data packet*. As a result, even if the Nonce values were compared to a moving window of valid values (which they are not), *Kiuchi* still does not disclose that the virtual private network is based on comparing a value in *each data packet* transmitted between the first computer and the second computer to a moving window of valid values, as claimed. One of ordinary skill in the art would not have considered *Kiuchi*’s C-HTTP requests and responses, which are application layer requests, to be data packets.

D. Claims 9, 25, and 40

31. I understand that claims 9, 25, and 40 recite that “the virtual private network is based on a comparison of a discriminator field in a header of *each data packet* to the secure computer network address to a table of valid discriminator fields,” emphasis added. I also understand that the Request asserts that a connection ID in *Kiuchi* corresponds to a “discriminator field,” and that two different *Kiuchi* passages each disclose the “comparison of a discriminator field in a header of each data packet . . . to a table of valid discriminator fields.” (Req. Ex. E-2 at 26.) I disagree.

32. First, the Request argues that *Kiuchi* discloses these claim features because a C-HTTP connection will be disconnected if a connection ID contained in a resource name is not found in a current connection table. (*Id.*) Specifically, *Kiuchi* explains that “[w]hen one of these resource names with a connection ID . . . is selected and requested by an end-user, the client-side proxy takes off the connection ID When the connection ID is not found in the current connection table in the client-side-proxy, the current connection is disconnected.” (*Kiuchi* 65.) But claims 9, 25, and 40

² Indeed, one of ordinary skill in the art at the time of the invention would have understood that in secure communications, a nonce is a unique, arbitrary number used only once to identify a particular communication.

recite a discriminator field “in a header of *each data packet*,” not a discriminator field constituting a portion of a resource name. Thus, the first passage of *Kiuchi* asserted by the Request does not describe anything corresponding to the recited “comparison of a discriminator field in a header of each data packet . . . to a table of valid discriminator fields.”

33. Second, the Request argues that the recited comparison is disclosed because *Kiuchi* explains that “if the server-side proxy detects that a given connection times out, it deletes the connection ID from the connection list, informing the client-side proxy that the connection is closed when an error status is returned in response to the request.” (Req. Ex. E-2 at 26, quoting *Kiuchi* 67.) But nowhere does *Kiuchi* teach that a connection ID is contained in *each data packet*, or that the virtual private network *is based on* a comparison of a discriminator field in a header of each data packet, as recited in the claims. Rather, the Request’s asserted passage suggests that the C-HTTP connection is, if anything, “based on” a timer, not on a connection ID. After all, the connection ID will endure beyond the termination of a C-HTTP connection until the server-side proxy eventually detects that the connection has already timed out. (*Kiuchi* 67.)

E. Claims 12 and 28

34. I understand that claims 12 and 28 recite that “the access request message contains a request for information stored at the secure computer network address.” I also understand that the Request asserts that *Kiuchi* discloses this feature because a server-side proxy may provide a connection ID and a second symmetric data exchange key to the client-side proxy. (Req. Ex. E-2 at 28.) I disagree.

35. *Kiuchi* discloses that the connection ID and second symmetric data exchange key are not *stored* at the secure computer network address, as recited in the claims, but rather are *newly generated* after the server-side proxy receives information regarding the client-side proxy from the C-HTTP name server. (*Kiuchi* 66.) Indeed, “[w]hen the server-side proxy obtains the client-side proxy’s [information], it . . . generates both a connection ID . . . and also a second symmetric data exchange key for response encryption, which are sent to the client-side proxy.” (*Id.*) Thus, the “request for connection” in *Kiuchi* alleged to correspond the “access request message” cannot contain a request for information stored at the server-side proxy, because that information, yet to be generated, is not stored at the server-side proxy at the time the message is sent.

F. Claims 13, 15, 29, and 31

36. I understand that claims 13 and 29 recite that the various features of claims 1 and 17 as occurring “at the client computer.” I also understand that claims 15 and 31 similarly recite “[t]he

method of claim 1, performed by a client computer.” I further understand that the Request asserts that in *Kiuchi*, “[t]he client-side proxy is the client computer as claimed.” (Req. Ex. E-2 at 29-30.) I disagree, because *Kiuchi* clearly distinguishes between clients and client-side proxies. (*Kiuchi* 64.)

37. Specifically, *Kiuchi* describes “user agents” as entities *within a firewall*, while explaining that the client-side proxy resides *on the firewall* of an institution, for example, a hospital. (*Id.*, explaining that the C-HTTP system *requires* “a client-side proxy on the firewall of one institution” and a server-side proxy on the firewall of another institution.) In fact, one of the explicit motivations for designing the C-HTTP system involving mandatory client-side and server-side proxies was the problem that “[i]t is not realistic for hospital information managers to expect that all *individual end-users*, including those who connect their PCs to in-hospital LANs, manage their keys in a secure manner.” (*Kiuchi* 68, emphasis added.)

38. A person of ordinary skill at the time of the invention would have been readily capable of distinguishing, as *Kiuchi* does, between client computers within an institutional firewall (e.g., a nurse’s or doctor’s PC in a hospital) and a computer residing on an institutional firewall (e.g., a client-side proxy). By asserting the equivalence of *Kiuchi*’s client-side proxy to a “client computer,” Requester ignores the fact that *Kiuchi* differentiates between its proxies and its end-user clients.

Truth and Accuracy of Statements

I further 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 ’180 patent.

Signed at New York, New York, this 16th day of December 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., Heraklion, Greece.
- **September 1991 - January 1993**
Member of the Technical Staff, Education Team, Computer Center of the University of Crete, Heraklion, 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 Symposium 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 (I²R), 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 Supérieure 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, Sinha 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 Information", 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 Sinha Sethumadhavan, Sal Stolfo, Junfeng Yang, and David August @ Princeton), "SPARCHS: Symbiotic, Polymorphic, Autonomic, 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, "*Snakeeyes*", 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 Honey Pots"
Michalis Polychronakis, Periklis Akrkitidis, Stelios Sidiroglou, Kostas G. Anagnostakis, Angelos D. Keromytis, and Evangelos Markatos. In *International Journal of Computer and Network Security (IJCNNS)*, 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. "AZM: 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 Monroe, 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"
Aleksy 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 Gateway"*
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"*
Sinha 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, Melbourne, 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. "*WebDAV: 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:

Victor Larson et al.	Control No.: 95/001,792
U. S. Patent No. 7,188,180	Group Art Unit: 3992
Issued: March 7, 2007	Examiner: Karin M. Reichle
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	Confirmation No. 1972

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. 7,188,180 ("the '180 patent"), which I understand is the subject of the above-identified reexamination proceedings. I am familiar with the '180 patent, including its claims.

3. Prior to and at the time of the inventions claimed in the '180 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 '180 patent and other patents in this family met this need. For instance, the inventions disclosed and claimed in the '180 patent include systems and methods of accessing a secure computer network address. As an example, independent claim 1 recites "receiving from [a] secure domain name service a response message containing [a] secure computer network address corresponding to [a] secure domain name; and sending an access request message to the secure computer network address using a virtual private network communication link." ('180 patent 56:56-61.) Independent claims 17 and 33 recite similar features. (*Id.* at 57:58-58:7, 59:13-29) Moreover, dependent claims 3 and 19 recite that "the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display." (*Id.* at 57:3-6, 58:17-21.) And, dependent claims 7, 23, and 38 recite that "the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer." (*Id.* at 57:19-23, 58:35-40, 60:16-20.)

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 '180 patent. (*Id.* at 1-4.) That is, they did not develop a solution that provided systems and methods of easily and conveniently accessing a secure computer network address.

6. As a second example of the long-felt need for the inventions of the '180 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 '180 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 '180 patent, SAIC would spend approximately \$2 million on internal research and development efforts. In the case of the technology claimed in the '180 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 '180 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 '180 patent, which provide systems and methods of accessing a secure computer network address, 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 '180 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 '180 patent. (*See* ¶¶ 4-5, *supra.*)

11. Additionally, as discussed above, no one had yet achieved the results of the claimed inventions of the '180 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 accessing a secure computer network address, the inventions of the '180 patent provided a solution for easily establishing virtual private network communication links without sacrificing security, thereby succeeding where others failed.

12. The claimed inventions of the '180 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 '180 patent. Microsoft has also entered into a similar license that includes the '180 patent. Microsoft entered into its license with VirnetX after it was found to have infringed the '180 patent and one other VirnetX patent 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 '180 patent. Likewise, on July 11, 2012, Mitel Networks Corporation entered into a license with VirnetX that also includes

the '180 patent. Then, on August 2, 2012, NEC Corporation and NEC Corporation of America entered into a license with VirnetX that also includes the '180 patent.

13. The claimed inventions of the '180 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 '180 patent, such as systems and methods of easily and conveniently accessing a secure computer network address. (Ex. B-5 at 1-2.)

15. The technology of the '180 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 '180 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 '180 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 '180 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 '180 patent.

Dated: December 18, 2012

By: /Robert Dunham Short III/
Robert Dunham Short III

APPENDIX - LIST OF EXHIBITS

EXHIBIT	DESCRIPTION
A-1	Verdict Form from <i>VirnetX, Inc. v. Microsoft Corp.</i> , No. 6:07-CV-80 (E.D. Tex. March 16, 2010).
A-10	Verdict Form from <i>VirnetX, Inc. v. Apple Inc.</i> , No. 6:10-CV-417 (E.D. Tex. Nov. 6, 2012).
A-11	Excerpted portions of Trial Transcript from <i>VirnetX, Inc. v. Apple Inc.</i> , No. 6:10-CV-417 (E.D. Tex. Nov. 5, 2012).
A-12	Slides from presentation entitled "C-HTTP The development of a secure, closed-HTTP-based network on the Internet," by T. Kiuchi, M.D., Dept. of Epidemiology and Biostatistics, University of Tokyo, Japan and S. Kaihara, M.D., Hospital Computer Center, University of Tokyo Hospital, Japan.
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, <i>Transient Partnerships Stretch Security Policy Management</i> , SIGNAL Magazine (Sept. 2001), http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes
B-4	Joel Snyder, <i>Living in Your Own Private Idaho</i> , Network World (January 26, 1998), http://www.networkworld.com/intranet/0126review.html
B-5	Tim Greene, <i>CEOs Chew the VPN Fat</i> , CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
Victor Larson et al.) Control No.: 95/001,792
U. S. Patent No. 7,188,180) Group Art Unit: 3992
Issued: March 6, 2007) Examiner: Deandra M. Hughes
For: METHOD FOR ESTABLISHING SECURE) Confirmation No. 1972
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 copies of the following documents:

1. Transmittal Letter (1 page);
2. Patent Owner's Response to Office Action (17 pages);
3. Declaration of Angelos D. Keromytis, Ph.D. (12 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; and
7. Certificate of Service (2 pages)

were served by first-class mail on December 19, 2012 on counsel for the third party Requester at the following address:

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 19, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14518695
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	19-DEC-2012
Filing Date:	25-OCT-2011
Time Stamp:	17:41:12
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	Trans Letter filing of a response in a reexam	Transmittal.pdf	45586 <small>9beafe51db5134b42ffc2029fd4c19e023ef98c7</small>	no	1

Warnings:

Information:

2	Response after non-final action-owner timely	Response.pdf	1272963	no	19
			b43d71e60b3c4c98ebaf4e5d81083affe17c25		
Warnings:					
Information:					
3	Reexam Miscellaneous Incoming Letter	KeromytisDec.pdf	3324973	no	45
			68c489f94caa263ff82e55f49adf0b75612fd407		
Warnings:					
Information:					
4	Reexam Miscellaneous Incoming Letter	ShortDecl.pdf	353765	no	5
			c25bd08dfefdbetd1876ee33d601093d612805dd		
Warnings:					
Information:					
5	Reexam Miscellaneous Incoming Letter	Appendix.pdf	56816	no	1
			7bb1e2b447bd2d46a6d06799c098c9cd1ab67164		
Warnings:					
Information:					
6	Reexam Miscellaneous Incoming Letter	ExhibitA1.pdf	96225	no	3
			224ebc119b90c42d1300a2e4c9b1809f0ebb6f3		
Warnings:					
Information:					
7	Reexam Miscellaneous Incoming Letter	ExhibitA10.pdf	91868	no	3
			3f535c1957068a9971f900bcd08f883e77e57101		
Warnings:					
Information:					
8	Reexam Miscellaneous Incoming Letter	ExhibitA11.pdf	150544	no	6
			e6ff7d3b1e769d06f3d971129e664713dfbea3c1		
Warnings:					
Information:					
9	Reexam Miscellaneous Incoming Letter	ExhibitA12.pdf	1060417	no	43
			eecf099f18131cea89452ef91aa3d1e3daded54f9		
Warnings:					
Information:					
10	Reexam Miscellaneous Incoming Letter	ExhibitB1.pdf	5956062	no	85
			24701c12e71bce8507ee4a52ea3b1c6f6b55bbf		
Warnings:					
Information:					

11	Reexam Miscellaneous Incoming Letter	ExhibitB2.pdf	6531212 1b50c62d7e38705d666b2a5274ab285b7073705	no	100
Warnings:					
Information:					
12	Reexam Miscellaneous Incoming Letter	ExhibitB3.pdf	390826 bca1a9da872889b5c1032f302df5f40d9f25b28c	no	5
Warnings:					
Information:					
13	Reexam Miscellaneous Incoming Letter	ExhibitB4.pdf	322450 a1198481beaa37ea50e2bbaa0201b5fed2b4b1d0	no	5
Warnings:					
Information:					
14	Reexam Miscellaneous Incoming Letter	ExhibitB5.pdf	343739 d7024955315e407faea552474deee61e3f221d59	no	6
Warnings:					
Information:					
15	Reexam Certificate of Service	Certificate.pdf	59551 3eacef520d45584c89cae0dd49a6d26af62b8c0a	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				20056997	
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the PETITION UNDER 37 CFR § 1.182 TO SHORTEN RESPONSE PERIODS AND ACCELERATE PROCEEDINGS was served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

the attorneys of record for the assignee of USP7921211 and of record for the assignee in the '1679, '1851, '1856, '1746, and '1792 reexamination proceedings, and on:

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington DC 20001

the attorneys of record for the assignee of USP 6502135, USP 7490151, USP 7418504, USP 6839759, and USP 7188180 and of record for the assignee in the '1714 reexamination proceeding, and on:

Sidley Austin LLP
1501 K Street N.W.
Washington, DC 20005

the attorneys of record for Apple Inc. in the merged '1714 and '1697 reexamination proceedings, all done in accordance with 37 CFR § 1.903, on December 5, 2012.

/David L. McCombs/

David L. McCombs,
Registration No. 32,271

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:	14389219
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	05-DEC-2012
Filing Date:	25-OCT-2011
Time Stamp:	14:19:38
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	747
Deposit Account	081394
Authorized User	MCCOMBS, DAVID L

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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Petition_to_Shorten.pdf	200572 28ab80f8745412b95b3969e459904e3f2ca b1ba4	yes	5
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Receipt of Petition in a Reexam	1	4	
		Reexam Certificate of Service	5	5	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30596 b4c606068b52e791e231fb90929e3735e55 47e24	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			231168		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor LARSON et al.) Control No.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 7, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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:

**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. 7,188,180 (“the ’180 patent”), hereby revokes all previous powers of attorney or authorization of agent granted in the ’180 patent before the date of execution hereof.

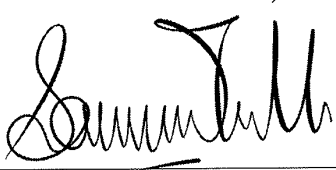
In compliance with 37 C.F.R. § 3.73(b), the undersigned verifies that VirnetX Inc. is the assignee of the entire right, title, and interest in the ’180 patent by virtue of an assignment recorded in the U.S. Patent and Trademark Office at Reel 018757, Frame 0326 on January 10, 2007.

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 '180 patent, including the reexamination proceedings assigned control no. 95/001,792, and in any other proceedings involving the '180 patent.

Please also send all future correspondence concerning the '180 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor LARSON et al.) Control Nos.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 7, 2007) Examiner: Karin M. Reichle
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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

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:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

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:	14369587
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./connie sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	03-DEC-2012
Filing Date:	25-OCT-2011
Time Stamp:	16:35:50
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_792.pdf	85659 <small>b5668c2d30f482bcc0737b7a17eb75479981e580</small>	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):		85659
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>		



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972

22852 7590 11/05/2012
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

HUGHES, DEANDRA M

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
11/05/2012	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.



DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NUMBER 95/001,792.

PATENT NUMBER 7,188,180.

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.

**Decision on Petition for Extension
of Time in Reexamination**

95/001,792

1. THIS IS A DECISION ON THE PETITION FILED: 31 October 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 19 September 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/
[Signature]

SPRS, AU 3992 Central Reexamination Unit
(Title)

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0005-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor LARSON et al.) Control No.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Deandra M. Hughes
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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:

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 the Director for a one-month extension of time for responding to the Office Action mailed September 19, 2012 ("Office Action") in the above-identified reexamination proceeding ("the '1,792 proceeding"). A response to the Office Action is currently due on November 19, 2012.

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 any deficiency to Deposit Account 06-0916.

VirnetX's counsel has begun preparing a response to the Office Action, but requests an extension of time of one month for the following reasons.

First, 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 the '504 patent; control nos. 95/001,789 and 95/001,856 involving U.S. Patent No. 7,921,211; and control no. 95/001,949 involving U.S. Patent No. 8,051,181. These proceedings will demand attention from VirnetX and strain its resources during the period for response to the Office Action. For example, the U.S. Patent and Trademark Office recently issued office actions in the '1,788, '1,789, '1,851, and '1,856 proceedings. These office actions currently have deadlines for response within the same timeframe as the deadline for responding to the instant Office Action, meaning that VirnetX must work to prepare all of these responses in parallel. Tending to these other proceedings while preparing a response to the instant Office Action will require, by any standard, a very significant amount of time and effort.

Additionally, VirnetX is working with a technical expert and expects to submit a declaration of the expert in support of its response to the Office Action. VirnetX is also working with the expert and investigating the need for supplemental declarations in responding to the office actions in the '1,788, '1,789, '1,851, and '1,856 proceedings. Thus, coordinating with the expert on multiple declarations in parallel will further require significant 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 November 19, 2012.

Attorney Docket No. 11798.0005-00000
Control No. 95/001,792

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 31, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0005-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
Victor LARSON et al.) Control No.: 95/001,792
U. S. Patent No. 7,188,180) Group Art Unit: 3992
Issued: March 6, 2007) Examiner: Deandra M. Hughes
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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 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 October 31, 2012, on counsel for the third party requester at the following address:

David L. McCombs, Esq.
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 31, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001792			
Filing Date:	25-Oct-2011			
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK			
First Named Inventor/Applicant Name:	7,188,180			
Filer:	Joseph Edwin Palys./Sandra Slayton			
Attorney Docket Number:	43614.100			
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:	14115941
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sandra Slayton
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	31-OCT-2012
Filing Date:	25-OCT-2011
Time Stamp:	15:36:21
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	2446
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1		Extension.pdf	155926	yes	4
			13ed44fa1c897c4c7938d34e73c2da4d42c18e1		
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Reexam Miscellaneous Incoming Letter	1	3	
		Reexam Certificate of Service	4	4	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30538	no	2
			c72308d2f5a09729cbd5e39a0ef2a8e551b5840d		
Warnings:					
Information:					
Total Files Size (in bytes):			186464		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

Re-Exam

RECEIVED

SEP 20 2012



CENTRAL REEXAMINATION UNIT

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re <i>Inter Partes</i> Reexamination of:)	
)	
Victor LARSON et al.)	Control No.: 95/001,792
)	
U. S. Patent No. 7,188,180)	Group Art Unit: 3992
)	
Issued: March 6, 2007)	Examiner: Deandra M. Hughes
)	
For: METHOD FOR ESTABLISHING)	Confirmation No. 1972
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

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 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 20, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

RECEIVED



SEP 20 2012

IDS Form PTO/SB/08: Substitute for form 1449A/PTO		Complete if Known	
CENTRAL REEXAMINATION UNIT INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>		Control Number	95/001,792
		Filing Date	December 25, 2011
		First Named Inventor	Victor Larson
		Art Unit	3992
		Examiner Name	Deandra M. Hughes
Sheet	1	of	52
		Attorney Docket Number	11798.0005

U.S. PATENTS						
Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code (if known)	MM-DD-YYYY		
		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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	2	of	52	<i>Attorney Docket Number</i>	11798.0005

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)			
		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				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number		95/001,792
				Filing Date		December 25, 2011
				First Named Inventor		Victor Larson
				Art Unit		3992
				Examiner Name		Deandra M. Hughes
Sheet	3	of	52	Attorney Docket Number		11798.0005

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		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	
				95/001,792	
				Filing Date	
				December 25, 2011	
				First Named Inventor	
Victor Larson					
Art Unit		3992			
Examiner Name		Deandra M. Hughes			
Sheet	4	of	52	Attorney Docket Number	
				11798.0005	

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	5	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>(if known)</i>			
		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				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number		95/001,792
				Filing Date		December 25, 2011
				First Named Inventor		Victor Larson
				Art Unit		3992
				Examiner Name		Deandra M. Hughes
Sheet	6	of	52	Attorney Docket Number		11798.0005

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 <i>(if known)</i>			
		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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	7	of	52	<i>Attorney Docket Number</i>	11798.0005

PUBLISHED U.S. PATENT APPLICATIONS						
Tab No.	Examiner Initials	Cite No.	Document Number	Issue or Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			Number-Kind Code (if known)	MM-DD-YYYY		
		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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	8	of	52	<i>Attorney Docket Number</i>	11798.0005

FOREIGN PATENT DOCUMENTS							
Tab	Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Translation
			Country Code Number Kind Code (if known)				
		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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	9	of	52	<i>Attorney Docket Number</i>	11798.0005

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 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.	
	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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	10	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation 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 Invalidation 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 Invalidation 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, <i>Personal Mobility For Multimedia Services In The Internet</i> , Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., <i>Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet</i> (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, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
				Attorney Docket Number	11798.0005
Sheet	11	of	52		

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, <i>The AltaVista Tunnel: Using the Internet to Extend Corporate Networks</i> , 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). (Goldschlag I, Onion Routing)	
	D55	Microsoft Corp., <i>Installing Configuring and Using PPTP with Microsoft Clients and Servers</i> (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., <i>IP Security for Microsoft Windows NT Server 5.0</i> (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., <i>Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services</i> (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., <i>Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead</i> (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., <i>Understanding Point-to-Point Tunneling Protocol PPTP</i> (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et al., <i>Protecting a Private Network: The AltaVista Firewall</i> , Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy <i>Implementation of Virtual Private Networks (VPNs) with IPSecurity</i> , <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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	12	of	52	<i>Attorney Docket Number</i>	11798.0005

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., <i>Virtual Private Networking An Overview</i> (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., <i>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</i> (1998) (available at http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxptrue). (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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	13	of	52	<i>Attorney Docket Number</i>	11798.0005

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., <i>Company Focuses on Quality and Customer Feedback</i> (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, <i>Domain Name System Security Extensions</i> , 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, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , <draft-ietf-dnsind-rrc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. <i>Virtual Private Networks</i> , 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," <i>Computer Networks</i> , 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	FreeSWAN Project, <i>Linux FreeS/WAN Compatibility Guide</i> (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			Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			<i>Control Number</i>	95/001,792
			<i>Filing Date</i>	December 25, 2011
			<i>First Named Inventor</i>	Victor Larson
			<i>Art Unit</i>	3992
			<i>Examiner Name</i>	Deandra M. Hughes
			<i>Attorney Docket Number</i>	11798.0005
Sheet	14	of	52	

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, <i>Distributing Kerberos KDC and Realm Information with DNS</i> <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). (Bhattacharya 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. <i>Check Point FireWall-1 Administration Guide</i> , 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, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , 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," <i>Mobile Computing and Communications Review</i> , 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	<i>Onion Routing</i> , "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	Publicly 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 <i>Gauntlet Firewall For Unix User's Guide Version 5.0</i> (1999). (Gauntlet User's Guide - Unix, Firewall Products)	
	D131	Network Associates <i>Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0</i> (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 (Use as many sheets as necessary)			Control Number	95/001,792	
			Filing Date	December 25, 2011	
			First Named Inventor	Victor Larson	
			Art Unit	3992	
			Examiner Name	Deandra M. Hughes	
Sheet	15	of	52	Attorney Docket Number	11798.0005

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 <i>Gauntlet Firewall For Unix Getting Started Guide Version 5.0</i> (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates <i>Release Notes Gauntlet Firewall for Unix 5.0</i> (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates <i>Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0</i> (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. <i>Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1</i> (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne <i>Dynamic Virtual Private Networks</i> (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred <i>Dynamic Virtual Private Networks (DVPN)</i> (December 21, 1999) (Kindred DVPN, DVPN)	
	D140	Dan Sterne <i>et al. TIS Dynamic Security Perimeter Research Project Demonstration</i> (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred <i>Dynamic Virtual Private Networks Capability Description</i> (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 <i>Security Quickstart Task Update</i> (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 <i>Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan</i> (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, <i>available at</i> 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, <i>available at</i> 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, <i>available at</i> 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) <i>available at</i> 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 (Use as many sheets as necessary)			Control Number	95/001,792	
			Filing Date	December 25, 2011	
			First Named Inventor	Victor Larson	
			Art Unit	3992	
			Examiner Name	Deandra M. Hughes	
Sheet	16	of	52	Attorney Docket Number	11798.0005

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), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) <i>available in</i> PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) <i>available in</i> PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) <i>available in</i> PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) <i>available in</i> PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) <i>available in</i> PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, <i>Essential Winlnet</i> 313-423 (Addison Wesley Longman 1998) (Essential Winlnet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) <i>available at</i> 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/technet/archives/winntas/proddocs/inetconctservice/bcgstart.msp (Internet Connection Services I)	
	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, <i>available at</i> http://www.microsoft.com/technet/archives/winntas/proddocs/inetconctservice/bcgstrtc.msp (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, <i>available at</i> http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.msp (IE5 Corporate Development)	
	D165	Mark Minasi, <i>Mastering Windows NT Server 4</i> 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	<i>Hands On, Self-Paced Training for Supporting Version 4.0</i> 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), <i>available at</i> http://www.microsoft.com/technet/archives/winntas/maintain/featusability/pptpwp3.msp (MS PPTP)	
	D168	Kenneth Gregg, <i>et al.</i> , <i>Microsoft Windows NT Server Administrator's Bible</i> 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), <i>available at</i> 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			Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			Control Number	95/001,792	
			Filing Date	December 25, 2011	
			First Named Inventor	Victor Larson	
			Art Unit	3992	
			Examiner Name	Deandra M. Hughes	
Sheet	17	of	52	Attorney Docket Number	11798.0005

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), <i>available at</i> 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, <i>available at</i> 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, <i>NT Network Plumbing: Routers, Proxies, and Web Services</i> 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, <i>available at</i> 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	
	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, <i>available at</i> 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, <i>F-Secure NameSurfer</i> (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, <i>F-Secure VPN Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	D177	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, <i>F-Secure SSH2.0 for Windows NT and 95</i> (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, <i>F-Secure VPN+ Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, <i>F-Secure VPN+ 4.1</i> (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, <i>F-Secure SSH</i> (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	D185	F-Secure, <i>F-Secure VPN+</i> (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, <i>F-Secure Management Tools, Administrator's Guide</i> (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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	18	of	52	Attorney Docket Number	11798.0005

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, <i>F-Secure Desktop, User's Guide</i> (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., <i>VPN Policy Manager</i> (January 2000) (VPN Policy Manager)	
	D189	F-Secure, <i>F-Secure VPN+ for Windows NT 4.0</i> (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., <i>SafeNet/Security Center Technical Reference Addendum</i> (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., <i>System Description for VPN Policy Manager and SafeNet/SoftPK</i> (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., <i>About SafeNet / VPN Policy Manager</i> (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., <i>Gauntlet Internet Firewall, Firewall Product Functional Summary</i> July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., <i>Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0</i> (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, <i>Windows NT Terminal Server and Citrix Metaframe</i> (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, <i>Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame</i> (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., <i>Securing L2TP using IPSEC</i> (February 2, 1999)	
	D198	156. <i>Finding Your Way Through the VPN Maze</i> (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, <i>The Business Case for Secure VPNs</i> (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., <i>WatchGuard LiveSecurity for MSS Powerpoint</i> (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., <i>MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes</i> (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., <i>MSS Firewall Specifications</i> (1999)	
	D204	WatchGuard Technologies, Inc., <i>Request for Information, Security Services</i> (2000)	
	D205	WatchGuard Technologies, Inc., <i>Protecting the Internet Distributed Enterprise, White Paper</i> (February 2000)	
	D206	Air Force Research Laboratory, <i>Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)</i> (January 29, 1998)	
	D207	Technologies, Inc., <i>WatchGuard Firebox System Powerpoint</i> (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA <i>Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0</i> (September 21, 1998)	
	D209	BBN Information Assurance Contract, <i>TIS Labs Monthly Status Report</i> (March 16-April 30, 1998)	
	D210	DARPA, <i>Dynamic Virtual Private Network (VPN) Powerpoint</i>	
	D211	GTE Internetworking, <i>Contractor's Program Progress Report</i> (March 16-April 30, 1998)	
	D212	Darrell Kindred, <i>Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization</i> (January 30, 2001)	
	D213	<i>Virtual Private Networking Countermeasure Characterization</i> (March 30, 2000)	
	D214	<i>Virtual Private Network Demonstration</i> (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 <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	19	of	52	Attorney Docket Number	11798.0005

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, <i>Dynamic Virtual Private Networks (VPNs) and Integrated Security Management</i> (2000)	
	D216	Information Assurance/NAI Labs, <i>Create/Add DVPN Enclave</i> (2000)	
	D217	NAI Labs, <i>IFE 3.1 Integration Demo</i> (2000)	
	D218	Information Assurance, <i>Science Fair Agenda</i> (2000)	
	D219	Darrell Kindred et al., <i>Proposed Threads for IFE 3.1</i> (January 13, 2000)	
	D220	<i>IFE 3.1 Technology Dependencies</i> (2000)	
	D221	<i>IFE 3.1 Topology</i> (February 9, 2000)	
	D222	Information Assurance, <i>Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development</i> January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation</i> (2000)	
	D224	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.2</i> (2000)	
	D225	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)	
	D226	T. Braun et al., <i>Virtual Private Network Architecture</i> , Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - <i>PGP Total Network Security Suite, Dynamic Virtual Private Networks</i> (1999)	
	D228	Microsoft Corporation, <i>Microsoft Proxy Server 2.0</i> (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., <i>A Guide To Microsoft Proxy Server 2.0</i> (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, <i>Setting Server Parameters</i> (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, <i>Microsoft Proxy Server 2</i> (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., <i>MCSE Proxy Server 2 Study Guide</i> (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, <i>IIS 4 and Proxy Server 2</i> (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, <i>MCSE Test Success: Proxy Server 2</i> (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, <i>The Windows NT and Windows 2000 Answer Book</i> (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (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	<i>AutoSOCKS v2. 1, Datasheet</i> , http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, <i>Use of DNS to Distribute Keys</i> , 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	20	of	52	<i>Attorney Docket Number</i>	11798.0005

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; <i>Extended VPN Uses The Internet to Create Virtual Private Networks</i> , 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 Kosior, "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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	21	of	52	<i>Attorney Docket Number</i>	11798.0005

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	22	of	52	<i>Attorney Docket Number</i>	11798.0005

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. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)	
	D292	DPCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages. 3 0	
	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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	23	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidation Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidation 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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	24	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	25	of	52	<i>Attorney Docket Number</i>	11798.0005

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	26	of	52	<i>Attorney Docket Number</i>	11798.0005

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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	27	of	52	Attorney Docket Number	11798.0005

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 <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	28	of	52	Attorney Docket Number	11798.0005

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 <i>(Use as many sheets as necessary)</i>			<i>Control Number</i>	95/001,792	
			<i>Filing Date</i>	December 25, 2011	
			<i>First Named Inventor</i>	Victor Larson	
			<i>Art Unit</i>	3992	
			<i>Examiner Name</i>	Deandra M. Hughes	
Sheet	29	of	52	<i>Attorney Docket Number</i>	11798.0005

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	30	of	52	Attorney Docket Number	11798.0005

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 <i>VirnetX v. Microsoft</i> .	
	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 <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	31	of	52	Attorney Docket Number	11798.0005

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 Accessible 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/rfc/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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	32	of	52	Attorney Docket Number	11798.0005

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://www.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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	33	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	34	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	35	of	52	Attorney Docket Number	11798.0005

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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	36	of	52	<i>Attorney Docket Number</i>	11798.0005

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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	37	of	52	<i>Attorney Docket Number</i>	11798.0005

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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	38	of	52	<i>Attorney Docket Number</i>	11798.0005

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, Gauntlet System and Gauntlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gauntlet System and Gauntlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gauntlet 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, Efilng 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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	39	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Astra Technologies Ltd, NEC Corporation, NEC Corporation of America and Astra USA, Inc.</i> , 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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	40	of	52	Attorney Docket Number	11798.0005

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 <i>VirnetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.</i> , 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, (November 1998) 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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	41	of	52	<i>Attorney Docket Number</i>	11798.0005

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 Invalidation 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	42	of	52	Attorney Docket Number	11798.0005

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	43	of	52	<i>Attorney Docket Number</i>	11798.0005

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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	44	of	52	Attorney Docket Number	11798.0005

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 <i>VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Astra Technologies Ltd, NEC Corporation, NEC Corporation of America and Astra USA, Inc.</i> , 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.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	45	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>Lendenmann</i> reference. The link to the <i>Lendenmann</i> 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	46	of	52	<i>Attorney Docket Number</i>	11798.0005

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 7,921,211 relative 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control Number	95/001,792
				Filing Date	December 25, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Deandra M. Hughes
Sheet	47	of	52	Attorney Docket Number	11798.0005

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 <i>Inter Partes</i> Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate <i>Inter Partes</i> Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate <i>Inter Partes</i> 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, <i>VirnetX, Inc. v. Microsoft Corp.</i> , 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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	48	of	52	<i>Attorney Docket Number</i>	11798.0005

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	49	of	52	<i>Attorney Docket Number</i>	11798.0005

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/annviewer.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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	50	of	52	<i>Attorney Docket Number</i>	11798.0005

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	51	of	52	<i>Attorney Docket Number</i>	11798.0005

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 <i>(Use as many sheets as necessary)</i>				<i>Control Number</i>	95/001,792
				<i>Filing Date</i>	December 25, 2011
				<i>First Named Inventor</i>	Victor Larson
				<i>Art Unit</i>	3992
				<i>Examiner Name</i>	Deandra M. Hughes
Sheet	52	of	52	<i>Attorney Docket Number</i>	11798.0005

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 VirnetX 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.

RECEIVED

SEP 20 2012

CENTRAL REEXAMINATION UNIT



PATENT
Customer No. 22,852
Attorney Docket No. 11798.0005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re <i>Inter Partes</i> Reexamination of:)	
)	
Victor LARSON et al.)	Control No.: 95/001,792
)	
U. S. Patent No. 7,188,180)	Group Art Unit: 3992
)	
Issued: March 6, 2007)	Examiner: Deandra M. Hughes
)	
For: METHOD FOR ESTABLISHING)	Confirmation No. 1972
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

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:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219-7672

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 20, 2012

By: Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972
22852	7590	09/19/2012	EXAMINER HUGHES, DEANDRA M	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413				
			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			09/19/2012	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.



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
HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Date:

MAILED

SEP 19 2012

CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792
PATENT NO. : 7188180
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)

INTER PARTES REEXAMINATION COMMUNICATION	Control No.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	DEANDRA M. HUGHES	3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

A SHORTENED STATUTORY PERIOD FOR RESPONSE TO THIS ACTION IS SET TO EXPIRE
 2 MONTH(S) THIRTY DAYS FROM THE MAILING DATE OF THIS LETTER. EXTENSIONS
OF TIME FOR PATENT OWNER ARE GOVERNED BY 37 CFR 1.956.

Each time the patent owner responds to this Office action, 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.

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.

Transmittal of Communication to Third Party Requester Inter Partes Reexamination	Control No.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	DEANDRA M. HUGHES	3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

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.

OFFICE ACTION IN INTER PARTES REEXAMINATION	Control No.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	DEANDRA M. HUGHES	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 17 January, 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 1,4,6-17,20,22-33,35 and 37-41 are subject to reexamination.
- 1b. Claims 2,3,5,18,19,21,34 and 36 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 1,4,6-17,20,22-33,35 and 37-41 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 _____

INTER PARTES REEXAMINATION NON-FINAL ACTION

1. This is a non-final action in the *inter partes* reexamination of **claims 1, 4, 6-17, 20, 22-33, 35 and 37-41** of USP 7,188,180. ("**180 patent**")

References Cited in Request

2. A total of two references, applied alone or in certain combinations, have been asserted in the request as providing teachings relevant to the claims of the '**180 patent**.

The references are as follows:

- (A) Kiuchi et al. "*The Development of a Secure, Closed HTTP-based Network on the Internet*", 1996. ("**Kiuchi**")
- (B) Martin, David M. "*A Framework for Local Anonymity in the Internet*", February 21, 2998. ("**Martin**")

Claim Rejections - 35 USC § 102

3. 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.

4. **Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, and 39-40** are rejected under 35 U.S.C. 102 (b) as being anticipated by **Kiuchi**.

As to these claims, the explanation of the rejections set forth in the request (pgs. 15-17) and claim charts (Exhibit E-2, pgs. 3-42), excluding the arguments as to the claim interpretation asserted in litigation, are incorporated here by reference.

Art Unit: 3992

Claim Rejections - 35 USC § 103

5. 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 negated by the manner in which the invention was made.

6. **Claims 11, 27, and 41** are rejected over 35 U.S.C. 103(a) as obvious over

Kiuchi.

As to these claims, the explanation of the rejections set forth in the request (pgs. 15-17) and claim charts (Exhibit E-2, pgs. 51-52), excluding the arguments as to the claim interpretation asserted in litigation, are incorporated here by reference.

7. **Claims 7, 23, and 38** are rejected over 35 U.S.C. 103(a) as obvious over **Kiuchi** in view of **Martin**.

As to these claims, the explanation of the rejections set forth in the request (pgs. 15-17) and claim charts (Exhibit E-2, pgs. 48-50), excluding the arguments as to the claim interpretation asserted in litigation, are incorporated here by reference.

Conclusion

8. All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: 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

Art Unit: 3992

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

9. 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.

10. Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties 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). PO extensions of time in *inter partes* reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for 3PR comments, because a comment period of 30 days from service of PO's response is set by statute. 35 U.S.C. 314(b)(3).

11. The PO is reminded of the continuing responsibility under 37 CFR 1.985(a) to apprise the Office of any litigation activity, or other concurrent proceeding, involving this patent throughout the course of this reexamination proceeding. The 3PR is also reminded of the ability to similarly apprise the Office of any such activity or proceeding

Art Unit: 3992

throughout the course of this reexamination proceeding. See MPEP §2686 and 2686.04.

12. Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.


Signed:

/Deandra M. Hughes/
Reexamination Specialist, Art Unit 3992

Conferees:

/Christina Y. Leung/
Reexamination Specialist, Art Unit 3992

/Daniel J Ryman/
Supervisory Patent Examiner, Art Unit 3992

Reexamination 	Application/Control No. 95001792	Applicant(s)/Patent Under Reexamination 7,188,180
	Certificate Date	Certificate Number

Requester Correspondence Address: **Patent Owner** **Third Party**

David L. McCombs
 HAYNES and BOONE LLP
 2323 Victory Avenue, Suite 700
 Dallas, TX 75219

LITIGATION REVIEW <input checked="" type="checkbox"/>	DMH (examiner initials)	08/25/2012 (date)
Case Name		Director Initials
Virnetx v. Cisco et al. 6:10cv417 (OPEN)		DJR & LY
Virnetx v. Microsoft 6:10cv94 (CLOSED)		↓
VirnetX v. Microsoft 6:07cv0080		↓

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

--	--



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972

22852 7590 09/06/2012

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

ART UNIT PAPER NUMBER

DATE MAILED: 09/06/2012

Please find below and/or attached an Office communication concerning this application or proceeding.



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
HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Date:

MAILED

SEP 06 2012

CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792
PATENT NO. : 7188180
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)



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

FINNEGAN, HENDERSON, FARBOW,
GARRETT & DUNNER, LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

(For Patent Owner)

MAILED

SEP 06 2012

CENTRAL REEXAMINATION UNIT

HAYNES AND BOONE LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

(For Third Party Requester)

In re Larson *et al.*

Inter Partes Reexamination Proceeding

Control No. 95/001,792

Filed: October 25, 2011

For: U.S. Patent No. 7,188,180

: DECISION ON

: PETITION UNDER

: 37 C.F.R. §§ 1.181 &

: 1.927

Third party requester filed a paper on January 17, 2012, entitled "Petition under 37 C.F.R. §§ 1.927 and 1.181" (hereinafter "the petition"). The petition is before the Director of the Central Reexamination Unit (CRU). Petitioner, the reexamination requester, seeks supervisory review of the order, which was mailed December 17, 2012, denying the request for *Inter Partes* Reexamination.

The petition is **GRANTED-IN-PART** for the reasons set forth below.

Art Unit: 3992

REVIEW OF RELEVANT FACTS

1. U.S. Patent No. 7,188,180 (“the ‘180 patent”) issued on March 6, 2007.
2. A request for *inter partes* reexamination was filed on December 8, 2009 for claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the ‘180 patent wherein the real party in interest was Microsoft Corporation. The reexamination proceeding was assigned Control No. 95/001,270 (hereinafter, the ‘270 proceeding).
3. An *inter partes* reexamination certificate issued on Jun. 7, 2011 in the ‘270 proceeding confirming claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the ‘180 patent as patentable.
4. A request for *inter partes* reexamination was filed on October 25, 2011 for claims 1-41 of the ‘180 patent by real party in interest Cisco Systems, Inc. The reexamination proceeding was assigned Control No. 95/001,792 (hereinafter, the ‘792 proceeding).
5. A determination denying the request for reexamination of claims 1-41 of the ‘180 patent was mailed on December 17, 2012 in the ‘792 proceeding.
6. The instant petition was filed on January 17, 2012.

RELEVANT PRIOR ART OF RECORD

1. Lendenmann, Rolf. Understanding OSF DCE 1.1 for AIX and OS/2, IBM International Technical Support Organization. October 1995. (“Lendenmann”)
2. Kiuchi et al. “*The Development of a Secure, Closed HTTP-based Network on the Internet*”, 1996. (“Kiuchi”)
3. Solana et al. “*Flexible Internet Secure Transactions Based on Collaborative Domains*”, 1997. (“Solana”)
4. Schimpf, Brian. “*Securing Web Access with DCE*”, February 10-11, 1997. (“Schimpf”)
5. Rosenberry et al. Understanding DCE. 1993. (“Rosenberry”)
6. Masys et al. “*Protecting Clinical Data on Web Client Computers: the PCASSO Approach*”, November 7-11, 1998. (“Masys”)
7. Martin, David M. “*A Framework for Local Anonymity in the Internet*”, February 21, 1998. (“Martin”)

Art Unit: 3992

Petitioner's Grounds in Support of the Requested Relief

Petitioner alleges that the examiner's denial of the request for reexamination is improper because the determination failed to sufficiently consider the interpretation of the claim terms 'secure domain name' and 'secure domain name service' that Patent Owner ("PO") asserted in litigation captioned VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION VS. MICROSOFT CORPORATION (hereafter "litigation").

Specifically, the petitioner argues that the examiner's determination is in error because the petitioner alleges that when the prior art is viewed against PO's asserted broadest reasonable interpretation in litigation, "... the prior art establishes a strong likelihood that the Requester will prevail against invalidating the claims" of the '180 patent. (See, e.g., Petition at 2-3).

DECISION**I. Standard of Review**

35 USC 312(c) and 37 CFR 1.927 provide for the filing of a petition to review an examiner's determination refusing to order *inter partes* reexamination. The CRU Director's review on petition is *de novo*. Therefore, the review will determine whether the examiner's refusal to order reexamination for claims 1-41 was correct, and will not necessarily indicate agreement or disagreement with every aspect of the examiner's rationale for the denial of the request to order reexamination for claims 1-41 of the '180 patent. The review will not consider evidence not of record at the time of the request for reexamination.

II. Relevant Regulations for *Inter Partes* Reexamination

37 C.F.R. § 1.913 states in part:

(a) Except as provided for in § 1.907 and in paragraph (b) of this section, any person other than the patent owner or its privies may, at any time during the period of enforceability of a patent which issued from an original application filed in the United States on or after November 29, 1999, file a request for *inter partes* reexamination by the Office of any claim of the patent on the basis of prior art patents or printed publications cited under § 1.501.

37 C.F.R. § 1.915(b) states in part:

(3) 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, and a detailed explanation of the pertinency and manner of applying the patents and printed publications to every claim for which reexamination is requested.

Art Unit: 3992

37 C.F.R. § 1.923 states:

Within three months following the filing date of a request for *inter partes* reexamination under § 1.915, the examiner will consider the request and determine whether or not the request and the prior art establish a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request. The examiner's determination will be based on the claims in effect at the time of the determination, will become a part of the official file of the patent, and will be mailed to the patent owner at the address as provided for in § 1.33(c) and to the third party requester. If the examiner determines that the request has not established a reasonable likelihood that the requester will prevail with respect to at least one of the challenged claims, the examiner shall refuse the request and shall not order *inter partes* reexamination.

37 C.F.R. § 1.927 states:

The third party 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 to order *inter partes* reexamination. Any such petition must comply with § 1.181(b). If no petition is timely filed or if the decision on petition affirms that a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request has not been established, the determination shall be final and non-appealable.

37 C.F.R. § 1.931(a) states:

If it is found that there is a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request, the determination will include an order for *inter partes* reexamination of the patent for resolution of the question of whether the requester will prevail.

III. The Legal Standard for Ordering Reexamination

A review of 35 USC 311-317 and 37 CFR 1.915, 1.919, and 1.923, after implementation of the Leahy-Smith America Invents Act¹, shows that *inter partes* reexamination of a United States Patent is only authorized when a consideration of prior art consisting of patents or printed publications establishes that there is a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request. In particular, 35 USC 311(a) requires that a request for *inter partes* reexamination be based upon prior art as set forth in 35 USC 301, that is, prior art consisting of patents or printed publications, while 37 CFR 1.915(b)(3) requires that a request for *inter partes* reexamination include "a statement ... showing that there is a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request."

Section 6(c)(3)(A) of the Leahy-Smith America Invents Act amended 35 USC 312 and 313 to delete any reference to the SNQ standard, and provide, in place of each deletion, language requiring the information presented in a request for *inter partes* reexamination (filed pursuant to

¹ Public Law 112-29, 125 Stat. 284 (2011).

Art Unit: 3992

35 USC 311) to show that there is a reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged in the request. With respect to the reasonable likelihood standard, House Rep. 112–98 (Part 1), 112th Cong., 1st Sess., provides, in connection with *inter partes* review, the following:

“The threshold for initiating an *inter partes* review is elevated from ‘significant new question of patentability’—a standard that currently allows 95% of all requests to be granted—to a standard requiring petitioners to present information showing that their challenge has a reasonable likelihood of success.” H.R. Rep. No. 112–98 (Part 1), at 47.

Similarly, with respect to the reasonable likelihood standard, a Senate debate in the Congressional Record at S1375 (March 8, 2011), 112th Cong., 1st Sess., provides, in connection with *inter partes* review, the following:

“Among the most important protections for patent owners added by the present bill are its elevated thresholds for instituting *inter partes* and post-grant reviews. The present bill dispenses with the test of “substantial new question of patentability,” a standard that currently allows 95% of all requests to be granted. It instead imposes thresholds that require petitioners to present information that creates serious doubts about the patent’s validity. ...

...The “reasonable likelihood” test is currently used in evaluating whether a party is entitled to a preliminary injunction, and effectively requires the petitioner to present a *prima facie* case justifying a rejection of the claims in the patent.”

To implement this change to the standard of granting an *inter partes* reexamination request, the Office revised the rules of practice for *inter partes* reexamination by amending 37 CFR 1.915, 1.923, 1.927, and 1.931 to delete any reference to the SNQ standard for granting reexamination, and insert in its place reference to the newly enacted “reasonable likelihood” standard. See “Revision of Standard for Granting an *Inter Partes* Reexamination Request: Final Rule,” 76 Fed. Reg. 59055 (Sept. 23, 2011). The relevant regulations, as amended, appear in subsection II.

In addition, the Patent Office must afford the claims the broadest reasonable interpretation consistent with the specification. *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). The legal standards for claim construction in reexamination do not necessarily correspond to the legal standards that are mandated to be used by the courts in litigation. See MPEP §2686.05 (determination of a substantial new question of patentability is made independently of a court's decision on validity because the District Courts and the Patent Office use different standards of proof and claim interpretation); see also *In re Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320,1321-22 (Fed. Cir. 1989) (during patent examination, the pending claims must be interpreted as broadly as their terms reasonably allow). As such, claim construction in litigation are not binding upon the Office and will not be explicitly discussed for the purposes of this *de novo* review of whether the proposed rejections of the request are reasonably likely to prevail against claims 1-41 of the ‘180 patent.

Art Unit: 3992

IV. Analysis of the Request for Reexamination of the '180 patent

Section 6(c)(3)(A) of the Leahy-Smith America Invents Act provides a provision under which a request for *inter partes* reexamination will not be granted unless the information presented in the request shows that there is a reasonable likelihood that the requester will prevail ("RLP") with respect to at least one of the claims challenged in the request. In order to show a RLP, the request, in view of the prior art, must set forth a proposed ground of rejection for a claim(s) that addresses each and every limitation set forth in the claim(s).

Points to be Reviewed

1. Whether Lendenmann establishes a RLP as to claims 1-41 as set forth in the request.
2. Whether Kiuchi establishes a RLP as to claims 1-41 as set forth in the request.
3. Whether Solana establishes a RLP as to claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 as set forth in the request.²
4. Whether Schimpf and Rosenberry establish a RLP as to claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 as set forth in the request.³

Point 1

Upon review of the request and claim charts, Requester proposed that Lendenmann teaches using 'secure domain names' such as names under the CCIT X.500 naming standard and the Internet Domain Name Service (DNS). (see e.g., Exhibit E-1 at 8) In addition, Requester proposed that Lendenmann's Cell Directory Service (CDS) reads on the claimed 'secure domain name service'. (see e.g., Exhibit E-1 at 11)

Upon review of the order, the examiner found that Lendenmann does not disclose the claimed 'secure domain name' and 'secure domain name service' because, *inter alia*, (1) the CCITT X.500 naming scheme is incompatible with the DNS naming scheme and (2) the name service of the Distributed Computing Environment (DCE) resolves names regardless of whether a CCITT X.500 name or a DNS name is provided. (Order at 4)

² Requester proposed a rejection of claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 under Solana. See page 24 of the request. Requester did not propose a rejection of claims 2-3, 5-9, 11, 13, 15-16, 18-19, 21-25, 27, 29, 31-32, 34, and 36-41 under Solana and as such, these claims will not be addressed in this decision.

³ Requester proposed a rejection of claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 over the combination of Schimpf and Rosenberry. See page 24 of the request. Requester did not propose a rejection of claims 2-3, 4-9, 11, 13, 15-16, 18-19, 21-25, 27, 29, 31-32, 34, and 36-41 over the combination of Schimpf and Rosenberry alone or in combination and as such, these claims will not be addressed in this decision.

Art Unit: 3992

In response to the examiner's findings, the petitioner argues the examiner failed to sufficiently consider the interpretation of the claim terms 'secure domain name' and 'secure domain name service' that PO asserted in litigation. Petitioner argues when Lendenmann is reviewed against PO's claim interpretation that is asserted in litigation, Lendenmann teaches the claimed 'secure domain name' and 'secure domain name service'. (Petition at 4-8)

First, for the reasons set forth above, the claim interpretation PO asserted in litigation will not be discussed in this *de novo* review of whether the proposed rejections over Lendenmann, alone or in combination, is likely to prevail against claims 1-41 of the '180 patent.

Second, the requirement that the request must present a RLP as to at least one claim places the initial burden of proof on the requester. Therefore, requester must have established a RLP showing that, as is presented in the request and claim charts, Lendenmann discloses, *inter alia*, the claimed: (1) 'secure domain name', (2) 'secure domain name service', and (3) 'virtual private network communication link'. (See e.g., Exhibit E-1 at 26).

Assuming, *arguendo*, that Lendenmann's disclosed X.500 domain name reads on the claimed 'secure domain name' and Lendenmann's disclosed CDS reads on the claimed 'secure domain service' then Lendenmann, as presented in the request and claim charts, does not disclose the claimed 'virtual private network communication link' of independent claims 1, 17, and 33. The request only relies upon Lendenmann to teach this claim limitation. (See, e.g. Exhibit E-1).

Since the claim term 'private' modifies the claim term 'network', a patent or printed publication must teach the privacy of the 'network' and not just the privacy of the 'communication link' in order to provide a reasonable likelihood of prevailing for the proposed rejection(s).

Here, the request and claim charts propose that the encrypted communication link of a remote procedure call ("RPC") reads on the claimed 'virtual private network communication link'. (See Exhibit E-1 at 21). The encrypted communication link of a RPC, however, does not teach the 'virtual private network communication link' because it pertains only to the privacy of the 'communication link' but does not address the privacy of the 'network'.

Accordingly, the request and claim charts do not support the required showing that there is a RLP against patent claims 1-41 over Lendenmann. Thus, the examiner correctly determined that there was no RLP as to Lendenmann, alone or in combination with another patent or printed publication.

Art Unit: 3992

Point 2

(A) Whether there is a RLP as to a proposed anticipation rejection of claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 under Kiuchi.⁴

Upon review of the request and claim charts, Requester proposed that Kiuchi's C-HTTP name reads on the claimed 'secure domain name' and that Kiuchi's C-HTTP name service reads on the claimed 'secure domain name service'. (See e.g., Exhibit E-2 at 5-8).

Upon review of the order, the examiner found that Kiuchi does not disclose the claimed 'secure domain name' and 'domain name service' because, *inter alia*, Kiuchi requires a host name which is associated with a secure computer, i.e. simultaneous host name resolution and host certification. (Order at 9).

In response to the examiner's findings, the petitioner argues that the examiner failed to appreciate that if the C-HTTP name is different, then a conventional DNS service will be unable to resolve the C-HTTP name. Petitioner argues that this asserted teaching of Kiuchi, when viewed in light of PO's own interpretative statements in the first reexamination, reads on the claimed 'secure domain name' and 'secure domain name service'. (Petition at 10-11).

As to the claimed 'secure domain name', it is found that Kiuchi's C-HTTP name reasonably anticipates this claim term because the disclosed C-HTTP name (e.g., Coordinating.Center.CSCRG hostname of server-side proxy disclosed in Appendix 3) is a non-standard domain name because the C-HTTP hostname is disclosed as "not necessarily the same as its DNS name" (e.g., see pg. 68, section 2: Name Service) and it is found that a query to a DNS would necessarily indicate that this C-HTTP hostname is unknown because .CSCRG is the unique name of the server at the hospital being queried by the client-side proxy at the University of Tokyo Branch Hospital.

As to the claimed 'secure domain name service', Kiuchi discloses that the DNS name service is not used for hostname resolution as the original secure name service, including certification, is used for the C-HTTP-based network. (pg. 64, section 2: Design and specification of C-HTTP). As such, it is found that Kiuchi's C-HTTP name service teaches the claimed 'secure domain name service' because Kiuchi specifically discloses that the C-HTTP name service is a secure name service.

Claims 1-2, 4-6, 8-10, and 12-16

As to claim 1, it is additionally found that Kiuchi teaches the other claim limitations in the general application of Kiuchi to claim 1, excluding the arguments as to the claim

⁴ This corresponds to the proposed rejection identified on page 23 of the request. The heading in Exhibit E-2 additionally includes claims 3 and 19 in the proposed anticipation rejection but the claim charts do not include a detailed explanation for claims 3 and 19 (see pages 19 and 34 of Exhibit E-2). Therefore, it is assumed that the heading of Exhibit E-2 contains a typographical error.

Art Unit: 3992

interpretation asserted in litigation, which is set forth in the request (pages 15-17) and claim charts. (Exhibit E-2 at 3-16) Therefore, it is found that requester has shown a RLP with respect to claim 1 for the proposed anticipation rejection under Kiuchi.

As to claim 2, it is found that the proposed rejection does not have a RLP for at least the reason that Kiuchi does not teach “automatically generating a secure domain name corresponding to a non-secure domain name”. The claim charts propose Kiuchi teaches this element because a secure domain name “may correspond to a ‘DNS’ name”. (Exhibit E-2 at 18) This anticipation rejection, however, does not have an RLP because a disclosure that a secure domain name may correspond to a ‘DNS’ name is neither an express or inherent disclosure as to the automatic generation of the secure domain name. In other words, there is no disclosure in Kiuchi as to the product of this alleged correspondence/generation.

As to claim 4, the proposed anticipation rejection under Kiuchi has a RLP because the general application of Kiuchi as to claim 4 in the request (pages 15-17) and claim charts (Exhibit E-2 at 19), excluding the arguments as to the claim interpretation asserted in litigation, appears to teach the claim limitations. Therefore, it is found that requester has shown a RLP with respect to claim 4 for the proposed anticipation rejection under Kiuchi.

As to claim 5, it is found that the proposed rejection does not have a RLP for at least the reason that Kiuchi does not teach “inserting one or more data values into each data packet sent to the secure computer network address” in combination with the other features of the claim. The claim charts propose that Kiuchi teaches this element because Kiuchi discloses “random bytes are inserted every fourth byte of the request and response”. (Exhibit E-2 at 21). This anticipation rejection, however, does not have an RLP because Kiuchi’s disclosure that “random bytes are inserted every fourth byte of the request and response” does not address the limitation requiring that the data values are inserted into *each* data packet sent to the secure network address because in Kiuchi random bytes are inserted only in the request and the response. Further, inserting a random byte in the request and response does not disclose inserting data values into the data packet *sent to the computer network address* because the request and response in Kiuchi is sent to/from the C-HTTP name server, which is not located at the claimed secure network address.

As to claims 6, 8-10, and 12-16, the proposed anticipation rejection under Kiuchi has a RLP because the general application of Kiuchi as to claim 4 in the request (pages 15-17) and claim charts (Exhibit E-2 at 21-33), excluding the arguments as to the claim interpretation asserted in litigation, appears to teach the claim limitations. Therefore, it is found that requester has shown a RLP with respect to claims 6, 8-10, and 12-16 for the proposed anticipation rejection under Kiuchi.

Art Unit: 3992

Claims 17-18, 20-22, 24-26, and 28-32

As to claim 17, it is additionally found that the proposed anticipation rejection of claim 17 under Kiuchi teaches the other claim limitations in the general application of Kiuchi to claim 17, excluding the arguments as to the claim interpretation asserted in litigation, which is set forth in the request (pages 15-17) and claim charts. (Exhibit E-2 at 31-33) Therefore, it is found that requester has shown a RLP with respect to claim 17 for the proposed anticipation rejection under Kiuchi.

As to claim 18, it is found that the proposed rejection does not have a RLP for at least the reason that Kiuchi does not teach “automatically generating a secure domain name corresponding to a non-secure domain name”. The claim charts propose that Kiuchi teaches this element because a secure domain name “may correspond to a ‘DNS’ name”. (Exhibit E-2 at 34). This anticipation rejection, however, does not have an RLP because a disclosure that a secure domain name may correspond to a ‘DNS’ name is neither an express or inherent disclosure as to the automatic generation of the secure domain name. In other words, there is no disclosure in Kiuchi as to the product of this alleged correspondence/generation.

As to claim 20, the proposed anticipation rejection under Kiuchi has a RLP because the general application of Kiuchi as to claim 20 in the request (pages 15-17) and claim charts (Exhibit E-2 at 34), excluding the arguments as to the claim interpretation asserted in litigation, appears to teach the claim limitations. Therefore, it is found that requester has shown a RLP with respect to claim 20 for the proposed anticipation rejection under Kiuchi.

As to claim 21, it is found that the proposed rejection does not have a RLP for at least the reason that Kiuchi does not teach “inserting one or more data values into each data packet sent to the secure computer network address” in combination with the other features of the claim. The claim charts propose that Kiuchi teaches this element because Kiuchi discloses “random bytes are inserted every fourth byte of the request and response”. (Exhibit E-2 at 34-35). This anticipation rejection, however, does not have an RLP because Kiuchi’s disclosure that “random bytes are inserted every fourth byte of the request and response” does not address the limitation requiring that the data values are inserted into *each* data packet sent to the secure network address because in Kiuchi random bytes are inserted only in the request and the response. Further, inserting a random byte in the request and response does not disclose inserting data values into the data packet *sent to the computer network address* because the request and response in Kiuchi is sent to/from the C-HTTP name server, which is not located at the claimed secure network address.

As to claims 22, 24-26, and 28-32, the proposed anticipation rejection under Kiuchi has a RLP because the general application of Kiuchi as to claims 22, 24-26, and 28-32 in the request (pages 15-17) and claim charts (Exhibit E-2 at 35-38), excluding the arguments as

Art Unit: 3992

to the claim interpretation asserted in litigation, appears to teach the claim limitations. Therefore, it is found that requester has shown a RLP with respect to claims 22, 24-26, and 28-32 for the proposed anticipation rejection under Kiuchi.

Claims 33-37 and 39-40

As to claim 33, it is additionally found that Kiuchi teaches the other claim limitations in the general application of Kiuchi to claim 33, excluding the arguments as to the claim interpretation asserted in litigation, which is set forth in the request (pages 15-17) and claim charts. (Exhibit E-2 at 31-33). Therefore, it is found that requester has shown a RLP with respect to claim 33 for the proposed anticipation rejection under Kiuchi.

As to claim 34, it is found that the proposed rejection does not have a RLP for at least the reason that Kiuchi does not teach “automatically generating a secure domain name corresponding to a non-secure domain name”. The claim charts propose that Kiuchi teaches this element because a secure domain name “may correspond to a ‘DNS’ name”. (Exhibit E-2 at 40). This anticipation rejection, however, does not have an RLP because a disclosure that a secure domain name may correspond to a ‘DNS’ name is neither an express or inherent disclosure as to the automatic generation of the secure domain name. In other words, there is no disclosure in Kiuchi as to the product of this alleged correspondence/generation.

As to claim 35, the proposed anticipation rejection under Kiuchi has a RLP because the general application of Kiuchi as to claim 35 in the request (pages 15-17) and claim charts (Exhibit E-2 at 41), excluding the arguments as to the claim interpretation asserted in litigation, appears to teach the claim limitations. Therefore, it is found that requester has shown a RLP with respect to claim 35 for the proposed anticipation rejection under Kiuchi.

As to claim 36, it is found that the proposed rejection does not have a RLP for at least the reason that Kiuchi does not teach “inserting one or more data values into each data packet sent to the secure computer network address” in combination with the other features of the claim. The claim charts propose that Kiuchi teaches this element because Kiuchi discloses “random bytes are inserted every fourth byte of the request and response”. (Exhibit E-2 at 41). This anticipation rejection, however, does not have an RLP because Kiuchi’s disclosure that “random bytes are inserted every fourth byte of the request and response” does not address the limitation requiring that the data values are inserted into *each* data packet sent to the secure network address because in Kiuchi random bytes are inserted only in the request and the response. Further, inserting a random byte in the request and response does not disclose inserting data values into the data packet *sent to the computer network address* because the request and response in Kiuchi is sent to/from the C-HTTP name server, which is not located at the claimed secure network address.

Art Unit: 3992

As to claims 37 and 39-40, the proposed anticipation rejection under Kiuchi has a RLP because the general application of Kiuchi as to claims 37 and 39-40 in the request (pages 15-17) and claim charts (Exhibit E-2 at 41-42), excluding the arguments as to the claim interpretation asserted in litigation, appears to teach the claim limitations. Therefore, it is found that requester has shown a RLP with respect to claims 37 and 39-40 for the proposed anticipation rejection under Kiuchi.

(B) Whether there is a RLP as to a proposed obviousness rejection of claim 3 and 19 over the combination of Kiuchi and Masys.

As to the proposed obviousness rejection of claims 3 and 19 over the combination of Kiuchi and Masys, it is not agreed that the proposed combination has a RLP for claims 3 and 19 for the following reasons.

First, for the reasons set forth above as to the anticipation rejection of base claims 2 and 18 over Kiuchi, Kiuchi does not teach “automatically generating a secure domain name corresponding to a non-secure domain name” in combination with the other features of the claims.

Second, Masys is not presented in the request (pages 15-17) and claim charts (Exhibit E-2 at 44-46), as teaching “automatically generating a secure domain name corresponding to a non-secure domain name”, which is found not to be taught by Kiuchi.

Therefore, the proposed obviousness rejection of claims 3 and 19, request (pages 15-17) and claim charts (Exhibit E-2 at 44-46), does not have a RLP because the combination does not teach “automatically generating a secure domain name corresponding to a non-secure domain name” in combination with the other features of the claims.

(C) Whether there is a RLP as to a proposed obviousness rejection of claims 7, 23, and 38 over the combination of Kiuchi and Martin.

As to the proposed obviousness rejection of claims 7, 23, and 38 over the combination of Kiuchi and Martin, the Office agrees that the proposed combination has a RLP against claims 7, 23, and 38 for the following reasons.

First, Martin appears to be analogous to Kiuchi because Martin pertains to a framework for local anonymity in the Internet and Kiuchi is directed to a closed HTTP based network for secure transfer of patient information for clinical use via the Internet.

Second, Martin teaches a technique for indirect connection addressing for the advantage of preserving the receiver anonymity in a locally anonymous network. (Martin at 9).

As such, the general application of the combination of Kiuchi and Martin, as asserted in the request (pages 15-17) and claim charts (Exhibit E-2 at 48-50), excluding the arguments as to

Art Unit: 3992

claim interpretation asserted in litigation, appears to teach the claim limitations because Kiuchi and Martin are printed publications that are analogous art and Martin teaches that which is absent in Kiuchi. Therefore, it is found that the request provides a RLP with respect to claims 17, 23, and 38 for the proposed obviousness rejection over the combination of Kiuchi and Martin.

(D) Whether there is a RLP as to a proposed obviousness rejection of claims 11, 27, and 41 over the Kiuchi alone.

As to the proposed obviousness rejection of claims 11, 27, and 41 over Kiuchi alone, the request (pages 15-17) and claim charts (Exhibit E-2 at 51-52), propose that choice of a top-level domain name such as .scom, .snet, .sorg, .sedu, .smil, or .sgov is a matter of design choice, and thus, renders the claims obvious.

It is agreed that this proposed obviousness rejection is supported by a RLP for claims 11, 27, and 41 because adding an 's' to indicate a secure domain to conventional domain names such as .com, .net, .org, .edu, .mil, or .gov is a design choice within the knowledge and skill in the art. In addition, the request sets forth a reasonable rationale for modifying Kiuchi because one of ordinary skill in this art would know that the added letter 's' stands for "security." Therefore, it is found that requester has shown a RLP with respect to the proposed obviousness rejection of claims 11, 27, and 41 over Kiuchi alone.

Point 3

Upon review of the request and claim charts, Requester proposed that Solana's DNS-sec X.509 reads on the claimed 'secure domain name'. (see e.g., Exhibit E-3 at 4).

Upon review of the order, the examiner found that Solana does not disclose the claimed 'secure domain name' because X.509 provides a digital certification authenticating the user of a name but does not provide a non-standard domain name which cannot be resolved by a conventional domain name service and results in a return message URL 'unknown'. (Order at 14).

In response to the examiner's findings, the petitioner argues that Solana provides examples of names that are not conventional domain names and that cannot be resolved by a conventional domain name service. Petitioner argues that this disclosure, in the view of PO's own interpretation of the claims that is asserted in litigation, reads on the claimed 'secure domain name'. (Petition at 11-12).

First, for the reasons set forth above, the claim interpretation PO asserted in litigation will not be discussed in this *de novo* review of whether the proposed rejections over Solana, alone or in combination, is likely to prevail against claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 of the '180 patent.

Art Unit: 3992

Second, the requirement that the request must present a RLP on at least one claim places the initial burden of proof on the requester. Therefore, requester must have established a RLP showing that, as is presented in the request and claim charts, Solana discloses, *inter alia*, the claimed (1) 'secure domain name' and (2) 'virtual private network communication link'. (See e.g., Exhibit E-3 at 17).

Assuming, *arguendo*, that Solana's X.509 reads on the claimed 'secure domain name' then Solana, as presented in the request and claim charts, does not disclose the claimed 'virtual private network communication link'.

Since the claim term 'private' modifies the claim term 'network', a patent or printed publication that is reasonably likely to prevail as an anticipatory reference against the claims of the '180 patent must anticipate the privacy of the 'network' and not just the privacy of the 'communication link'.

Here, the request and claim charts propose that the encrypted communication link between the initiator and responder reads on the claimed 'virtual private network communication link'. (Exhibit E-3 at 9) The encrypted communication link between initiator and responder, however, is not reasonably likely to anticipate the 'virtual private network communication link' because it pertains only to the privacy of the 'communication link' but does not address the privacy of the 'network'. In addition, Solana's reference to Virtual Private Networks in page 38 does not read on the claimed 'virtual private network communication link' because this reference does not pertain to the communication between Solana's initiator and responder but rather refers to one approach in a list of approaches that have failed to achieve an approved, universally accepted solution. (Solana at 38)

Accordingly, the request and claim charts do not support the required showing of unpatentability to the extent that there was a RLP as to claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 over Solana. Thus, the examiner correctly determined that there was no RLP as to Solana, alone or in combination with another patent or printed publication.

Point 4

Upon review of the request and claim charts, Requester proposed that the combination of Schimpf and Rosenberry makes obvious, *inter alia*, independent claims 1, 17, and 33 of the '180 patent. (see Exhibit E-3) Specifically, Requester proposes Schimpf's disclosed DCE CDS object name in the URL reads on the claimed 'secure domain name'. (Exhibit E-4 at 4-5) Also, Requester asserts Rosenberry provides examples of DCE CDS object names. (Id.) Further, Requester proposes Rosenberry discloses a cell directory service (CDS), which teaches the claimed 'secure domain name service'. (Exhibit E-4 at 7)

Upon review of the order, the examiner found that Schimpf does not disclose the claimed 'secure domain name' because the CDS, X.500, or a DNS naming scheme will not be resolved by a server of another naming scheme component (e.g. DNS or X.500) regardless of

Art Unit: 3992

whether it is a secure/non-standard domain name or a non-secure/standard domain name because the naming scheme is incompatible with the other components of the naming schemes. (Order at 14) The examiner also found that the name service of DCE resolves names regardless of whether a name provided, i.e. conventions and syntax requirements thereof, enforce/reflect any of the naming schemes and as such Rosenberry does not teach the claimed 'secure domain name service'. (Order at 15-16)

In response to the examiner's findings, the petitioner argues that the combination of Schimpf and Rosenberry, considered in the view of PO's own interpretation of the claims that is asserted in litigation, teach the critical limitations. (Petition at 13)

First, for the reasons set forth above, the claim interpretation PO asserted in litigation will not be discussed in this *de novo* review of whether the proposed rejections over Schimpf and Rosenberry, alone or in combination, is likely to prevail against claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 of the '180 patent.

Second, the requirement that the request must present a RLP on at least one claim places the initial burden of proof on the requester. Therefore, requester must have established a RLP showing that, as is presented in the request and claim charts, Schimpf in combination with Rosenberry discloses, *inter alia*, the claimed: (1) 'secure domain name', (2) 'secure domain name service' and (3) 'virtual private network communication link'. (See e.g., Exhibit E-4 at 4, 10-11)

Assuming, *arguendo*, that the combination of Schimpf and Rosenberry disclose the claimed 'secure domain name' and 'secure domain name service', then this combination, as presented in the request and claim charts, does not disclose the claimed 'virtual private network communication link' of independent claims 1, 17, and 33. The request only relies upon Lendenmann to teach this claim limitation. (See, e.g. Exhibit E-4).

Since the claim term 'private' modifies the claim term 'network', a patent or printed publication must teach the privacy of the 'network' and not just the privacy of the 'communication link' in order to provide a reasonable likelihood of prevailing for the proposed rejection(s).

Here, the request and claim charts propose that the encrypted secure local proxy ("SLP") reads on the claimed 'virtual private network communication link'. (Exhibit E-4 at 10-12) The encrypted SLP between client and server, however, does not teach the 'virtual private network communication link' because it pertains only to the privacy of the SLP (i.e., the 'communication link') but does not address the privacy of the 'network'.

Accordingly, the request and claim charts do not support the required showing of unpatentability to the extent that there was a RLP as to claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 over the combination of Schimpf and Rosenberry with or Solana. Thus, the

Art Unit: 3992

examiner correctly determined that there was no RLP as to the combination of Schimpf and Rosenberry, alone or in combination with another patent or printed publication.

SUMMARY

The *de novo* review on the record of the request for reexamination in the '792 reexamination proceeding, undertaken in light of the arguments presented in the petition, supports the determination that the request for reexamination has established that there is a reasonable likelihood that the requester will prevail as to the following proposed rejections:

- Claims 1, 4, 6, 8-10, 12-17, 20, 22, 24-26, 28-33, 35, 37, and 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b). [Part of proposed rejection #5 on page 23 of the request].
- Claims 7, 23, and 38 are obvious over Kiuchi and Martin over 35 U.S.C. § 103(a). [Proposed rejection #7 on page 23 of the request].
- Claims 11, 27, and 41 are obvious over Kiuchi alone over 35 U.S.C. § 103(a). [Proposed rejection #8 on page 24 of the request].

As such, these proposed rejections will be addressed in the non-final action, which will follow in due course.

The *de novo* review on the record of the request for reexamination in the '792 reexamination proceeding, undertaken in light of the arguments presented in the petition, supports the determination that the request for reexamination has not established that there is a reasonable likelihood that the requester will prevail as to the following proposed rejections:

- Claims 1-41 are anticipated by Lendenmann under 35 U.S.C. § 102(b) or render obvious under 35 U.S.C. § 103(a) by Lendenmann and secondary references. [Proposed rejections #1-4 on page 23 of the request].
- Claims 2, 5, 18, 21, 34, and 36 are anticipated by Kiuchi under 35 U.S.C. § 102(b). [Part of proposed rejection #5 on page 23 of the request].
- Claims 3 and 19 are obvious over Kiuchi and Masys under 35 U.S.C. § 103(a). [Proposed rejection #6 on page 23 of the request].
- Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 are anticipated by Solana under 35 U.S.C. § 102. [Proposed rejection #9 on page 24 of the request].
- Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103(a). [Proposed rejection #10 on page 24 of the request].

As such, these proposed rejections will not be addressed in the non-final action.

Art Unit: 3992

CONCLUSION

1. Based on a *de novo* review of the record as a whole, the PETITION is **GRANTED-IN-PART**.
2. Requester has established there is a reasonable likelihood of prevailing with respect to claims 1, 4, 6-17, 20, 22-33, 35, and 37-41 of the '180 patent and reexamination is ordered for these claims.
3. Requester has not established there is a reasonable likelihood of prevailing with respect to claims 2-3, 5, 18-19, 21, 34, and 36 of the '180 patent and reexamination is not ordered for these claims.
4. The examiner assignment of the ordered reexamination proceeding will be made pursuant to MPEP 2648. The examiner will issue a first Office action on the merits in due course.
5. This decision is final and non-appealable. 37 CFR 1.927. No further communication on this matter will be acknowledged or considered.
6. Telephone inquiries related to this decision should be directed to Mark Reinhart, Supervisory Patent Examiner, at (571) 272-1611.



Irem Yucel
Director
Central Reexamination Unit



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972
22852	7590	02/10/2012	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			ART UNIT	PAPER NUMBER

DATE MAILED: 02/10/2012

Please find below and/or attached an Office communication concerning this application or proceeding.



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
HAYNES AND BOONE, LLP
IP SECTION
2233 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

MAILED

Date: FEB 10 2012

CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792
PATENT NO. : 7188180
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)



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

Joseph E. Palys :
FINNEGAN, HENDERSON, FARABOW, : (For Patent Owner)
GARRETT & DUNNER LLP :
901 New York Avenue, N.W. :
Washington, D.C.. 20001-4413 :

MAILED

FEB 10 2012

CENTRAL REEXAMINATION UNIT

David L. McCombs :
HAYNES AND BOONE LLP : (For Third Party Requester)
2323 Victory Ave., Suite 700 :
Dallas, Texas 75219 :

In re: Larson et al. : DECISION ON PETITION TO VACATE
Inter Partes Reexamination Proceeding : FILING DATE OF *INTER PARTES*
Control No.: 95/001,792 : REEXAMINATION PROCEEDING
For: U.S. Patent No. 7,188,180 : AND PETITION IN OPPOSITION THEREOF

This is a decision on the 17 November 2011 petition filed by the patent owner under 37 CFR 1.181 entitled "Petition to Vacate *Inter Partes* Reexamination" [hereinafter "petition to vacate"] and the 1 December 2011 petition filed by the third party requester under 37 CFR 1.182 entitled "Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination" [hereinafter "petition in opposition"]. The petition to vacate requests that the Office vacate the filing date of the reexamination proceeding because the request for reexamination is not based on prior art patents or printed publications.

The petition in opposition is being treated as a petition under 37 CFR 1.181. As such, these petitions are before the Director of the Central Reexamination Unit.

The petition to vacate is dismissed for the reasons set forth below.

The petition to oppose is dismissed for the reasons set forth below.

REVIEW OF RELEVANT FACTS

- U.S. Patent No. 7,188,180 [hereinafter “180 patent”] was granted to Larson et al. on 6 March 2007.
- On 25 October 2011, a request for *inter partes* reexamination was filed by a third party requester. The resulting reexamination proceeding was assigned control number 95/001,792 [hereinafter “the ‘1792 proceeding”].
- On 17 November 2011, patent owner filed the petition to vacate.
- On 1 December 2011, the third party requester filed the petition in opposition.

STATUTES, REGULATIONS, AND PATENT EXAMINING PROCEDURES

37 CFR 1.4 Nature of Correspondence and Signature Requirements

- (c) Since different matters may be considered by different branches or sections of the United States Patent and Trademark Office, each distinct subject, inquiry or order must be contained in a separate paper to avoid confusion and delay in answering papers dealing with different subjects.

37 CFR 1.181 Petition to the Director

- (a) Petition may be taken to the Director:
 - (1) From any action or requirement of any examiner in the *ex parte* prosecution of an application, or in *ex parte* or *inter partes* prosecution of a reexamination proceeding which is not subject to appeal to the Board of Patent Appeals and Interferences or to the court.

37 CFR 1.939 Unauthorized Papers in *Inter Partes* Reexamination

- (a) If an unauthorized paper is filed by any party at any time during the *inter partes* reexamination proceeding it will not be considered and may be returned.
- (b) Unless otherwise authorized, no paper shall be filed prior to the initial Office action on the merits of the *inter partes* reexamination.

MPEP § 2625 Untimely Paper Filed Prior to First Office Action

Pursuant to 37 CFR 1.939, after filing of a request for inter partes reexamination, no papers directed to the merits of the reexamination other than (A) citations of patents or printed publications under 37 CFR 1.501 and 1.933, (B) another complete request under 37 CFR 1.510 or 37 CFR 1.915, or (C) notifications pursuant to MPEP § 2686, should be filed with the Office prior to the date of the first Office action in the reexamination proceeding. Any papers directed to the merits of the reexamination, other than those under 37 CFR 1.501, 1.933, 1.510 or 1.915, or under MPEP § 2686, filed prior to the date of the first Office action will be returned to the sender without consideration. If the papers are entered prior to discovery of the impropriety, such papers will be expunged from the record. A copy of the letter providing notification of the returned papers or expungement will be made of record in the patent file. However, no copy of the returned/expunged papers will be retained by the Office.

DECISION ON PETITION TO VACATE THE FILING DATE

Patent owner filed this petition to vacate after the filing of the request for *inter partes* reexamination but prior to the date of the first Office action in the reexamination proceeding. Although page 1 of the petition contains a statement that relief is sought under 37 CFR 1.183 for entry of the petition, the petition is being addressed solely under 37 CFR 1.181. The patent owner's combined petition under 37 CFR 1.181 and 1.183 is deemed improper because it combines two distinct petitions, which is not compliant with 37 CFR 1.4. The relief requested under 37 CFR 1.183 is procedurally dismissed under 37 CFR 1.4.

The MPEP clearly states that “[p]ursuant to 37 CFR 1.939, after filing of a request for *inter partes* reexamination, no papers directed to the merits of the reexamination other than [for certain limited exceptions] should be filed with the Office prior to the date of the first Office action in the reexamination proceeding.” MPEP 2625. These exceptions include “(A) citations of patents or printed publications under 37 CFR 1.501 and 1.933, (B) another complete request under 37 CFR 1.510 or 37 CFR 1.915, [and] (C) notifications pursuant to MPEP 2686.” *Id.*

In this case, the petition to vacate is directed to the merits of the reexamination because it discusses whether the request for reexamination is based on printed publications, which is an appealable matter according to MPEP 2646(II). The MPEP goes on to point out that such a matter “can be argued by the patent owner and appealed during the examination phase of the reexamination proceeding.” *Id.* Therefore, the issues concerning whether or not a document is a

printed publication are not appropriate to address via a petition even if filed after the first Office action.

In addition, the petition to vacate does not fall within one of the enumerated exceptions listed in MPEP § 2625. The petition to vacate does not constitute a citation of patents or printed publications under 37 CFR 1.501 and 1.933. The petition to vacate does not constitute another complete request under 37 CFR 1.510 or 37 CFR 1.915. Finally, the petition to vacate is not a notification pursuant to MPEP § 2686.

Since the petition to vacate goes to the merits of the case and since the petition to vacate does not fall within one of the exceptions enumerated in MPEP § 2625, the petition is an unauthorized or improper paper under 37 CFR 1.939.

This petition is **dismissed** as being an improper paper.

DECISION ON PETITION IN OPPOSITION

The third party requester filed the petition in opposition to oppose the petition to vacate. The filing of the petition occurred after the filing of the request for *inter partes* reexamination but prior to the date of the first Office action in the reexamination proceeding. Since the petition to vacate is improper, there is no petition filed under 37 CFR 1.181 upon which the third party requester may base the filing of the single submission in opposition. In addition, the petition in opposition is directed to the merits of the reexamination for the same reasons discussed above regarding the petition to vacate. Finally, the petition in opposition also does not fall within one of the enumerated exceptions set forth above.

Since the petition in opposition goes to the merits of the case and since the petition in opposition does not fall within one of the exceptions enumerated in MPEP § 2625, the petition in opposition is deemed an unauthorized or improper paper under 37 CFR 1.939.

This petition is **dismissed** as being an improper paper.

In view of the above, the present petitions in the reexamination proceeding do not have an entry right under the rules. Therefore, the present petitions will be expunged from record in the '1788 reexamination proceeding, and are being returned to the petitioners ***without consideration of the substance of the petitions***. As the petitions has been entered into the electronic Image File Wrapper (IFW) record, the petitions will be "returned" by closing the paper in the IFW, and marking the paper nonpublic to expunge it from the record. The present decision will, however, be made of record in the reexamination proceeding. See also MPEP § 2625.

CONCLUSION

1. The patent owner's petition under 37 CFR 1.181 to vacate the reexamination proceeding is hereby **dismissed**.
2. The third party requester's petition in opposition is hereby **dismissed**.
3. The patent owner's petition under 37 CFR 1.181 and third party requester's petition in opposition **will be expunged** from the record by closing the papers in the IFW record, and marking the papers nonpublic. This decision, however, will be of record in the proceeding.
4. The reexamination proceeding will be returned to the examiner to act on the request for reexamination.
5. Any response should be addressed as follows:

By Mail to: Mail Stop *Inter Partes* 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: Registered users of EFS-Web may alternatively submit such correspondence via 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.

6. Telephone inquiries with regard to this decision should be directed to Matthew Brooks, SPE AU 3992, at (571)272-8112, in the event that Matthew Brooks is unavailable, to the undersigned at (571) 272-0700.



Irem Yucel
Director, Central Reexamination Unit



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.
95/001,792	10/25/2011	7,188,180	43614.100	1972

22852 7590 02/10/2012

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

ART UNIT PAPER NUMBER

DATE MAILED: 02/10/2012

Please find below and/or attached an Office communication concerning this application or proceeding.



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
HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Date:

MAILED
FEB 10 2012
CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792
PATENT NO. : 7188180
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)



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

Joseph E. Palys
FINNEGAN, HENDERSON, FARABOW : (For Patent Owner)
GARRETT & DUNNER, LLP :
901 New York Avenue, N.W. :
Washington, D.C. 20001-4413 :

MAILED

FEB 1 0 2012


CENTRAL REEXAMINATION UNIT

David L. McCombs :
HAYNES AND BOONE, LLP : (For Third Party Requester)
2323 Victory Ave., Suite 700 :
Dallas, TX 75219 :

In re Larson et alia : DECISION VACATING
Inter partes Reexamination Proceeding : PETITION DECISION MAILED
Control No. 95/001,792 : 30 DECEMBER 2011
Filed: 25 October 2011 :
For U.S. Patent No. 7,188,180 :

Upon review of the petition decision, mailed 30 December 2011, it has been discovered that the petition decision was unsigned when it was mailed. Therefore, this communication is hereby vacated and expunged from the record by being designated "closed" and "not public". The communication will form no part of the record and will not be available to the public. This decision will be made of record in the reexamination file.

SUMMARY: The petition decision *Inter Partes* Reexamination 95/001,792, mailed 30 December 2011, has been vacated.


Irem Yucel,
Director, CRU 3992
571-272-0700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Reexamination Control No.: 95/001,792	§	Attorney Docket No.: 43614.100
	§	
Patent No.: 7,188,180	§	Customer No.: 27683
	§	
For: METHOD FOR ESTABLISHING	§	Real Party In Interest:
SECURE COMMUNICATION LINK	§	Cisco Systems, Inc.
BETWEEN COMPUTERS OF	§	
VIRTUAL PRIVATE NETWORK	§	
	§	
Examiner: Karin M. Reichle	§	
	§	
Art Unit: 3992	§	Conf. No. 1972

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

PETITION UNDER 37 C.F.R. §§ 1.927 and 1.181

I. Introductory Remarks

Requester hereby petitions under the provisions of 37 C.F.R. §§ 1.927 and 1.181 for a review of the reexamination Examiner's decision that the prior art references identified in the Request for *Inter Partes* Reexamination filed on October 25, 2011 ("the Request") do not establish a reasonable likelihood that Requester will prevail with respect to claims 1-41 of U.S. Patent No. 7,188,180 ("the '180 patent"). The decision denying the Request stated that the prior art references failed to teach a "secure domain name" and a "secure domain name service" as recited in the claims. But those statements failed to sufficiently consider the Patent Owner's broad interpretation of these terms. Accordingly, Requester requests that the Director reconsider the Request and order reexamination of claims 1-41.

II. Statement of Facts

1. The '180 patent issued on March 6, 2007 with 41 claims.

2. On December 8, 2009, Microsoft Corp. filed a Request for *Inter Partes* Reexamination of the '180 patent. The Request was granted and assigned Control No. 95/001,270.
3. On June 7, 2011, the Office issued an Inter Partes Reexamination Certificate confirming all claims that had been subject to Reexamination Control No. 95/001,270.
4. On October 25, 2011, Requester filed a Request for *Inter Partes* Reexamination of the '180 patent.
5. Reexamination was requested for all 41 issued claims of the '180 patent based on four primary references: (1) Rolf Lendenmann, "Understanding OSF DCE 1.1 For AIX and OS/2," (2) Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet," (3) Eduardo Solana and Jurgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains," and (4) the combination of Brian C. Schimpf, "Secure Web Access with DCE," and Ward Rosenberry, et al., "Understanding DCE." Additional references were provided with respect to limitations recited in dependent claims.
6. In an Order dated December 17, 2011, the reexamination Examiner found that none of the references, alone or in proposed combinations, establish a reasonable likelihood that Requester will prevail with respect to claims 1-41 of the '180 patent.

III. Overview

The '180 Patent is generally directed to accessing a secure computer network using a secure domain name. The patent describes using a "secure domain name service" to resolve a "secure domain name" to a network address.

During the Microsoft-initiated reexamination, the Patent Owner overcame the prior art by providing a distinguishing interpretation of the claim terms "secure domain name" and "secure domain name service":

Further, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain

name that happens to correspond to a secure computer... For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*).¹

Thus, the Patent Owner defined the term “secure domain name” in the negative—that is, by stating only that it cannot be resolved by conventional domain name server. The Patent Owner asserts that the term encompasses any name that is not a conventional domain name.

In declining the order reexamination, the examiner failed to consider the Patent Owner’s own interpretation of the claims. When the prior art is reviewed against the Patent Owner’s asserted broadest reasonable interpretation, the prior art establishes a strong likelihood that the Requester will prevail in invalidating the claims. Thus, reexamination should be ordered for claims 1-41.

IV. Points to be Reviewed

Point 1. Whether Lendenmann establishes a likelihood that Requester will prevail with respect to claims 1-41 as set forth in the Request.

Point 2. Whether Kiuchi establishes a likelihood that Requester will prevail with respect to claims 1-41 as set forth in the Request.

Point 3. Whether Solana establishes a likelihood that Requester will prevail with respect to claims 1-41 as set forth in the Request.

Point 4. Whether Schimpf and Rosenberry establish a likelihood that Requester will prevail with respect to claims 1-41 as set forth in the Request.

¹ Reexamination Control No. 95/001,270, Action Closing Prosecution at 3 (Jun. 16, 2010).

V. Remarks in Support of Actions Requested

The following remarks set forth and discuss points overlooked by the reexamination Examiner in evaluating the prior art and the claims under the Patent Owner's asserted broadest reasonable interpretation.

A. Patent Owner Asserts a Broad Interpretation of "Secure Domain Name" and "Secure Domain Name Service"

In interpreting the claim terms "secure domain name" and "secure domain name service," the Order Denying Reexamination refers repeatedly to statements in the previous reexamination of the '180 patent, but then fails to apply them. In the previous reexamination, the Patent Owner asserted—and the Patent Office agreed—that a secure domain name is identified by the fact that it "cannot be resolved by a conventional domain name service"²:

The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown.³

The Patent Owner asserted, and the Patent Office agreed, that the corresponding term "secure domain name service" was something that *can* resolve a secure domain name:

Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a

² Reexamination Control No. 95/001,270, Response at 6 (Apr. 19, 2010).

³ Reexamination Control No. 95/001,270, Action Closing Prosecution at 3 (Jun. 16, 2010).

conventional domain name service cannot resolve addresses for a secure domain name.⁴

Thus, the previous reexamination interpreted these terms by stating what they are not—specifically, that a “secure domain name” is not a standard domain name resolvable by a conventional domain name server. A “secure domain name service” is capable of resolving names that cannot be resolved by a conventional domain name server.

The Patent Owner applies these claim interpretations literally. According to the Patent Owner, *anything* which is not a conventional domain name may be a “secure domain name.” For example, at trial in the case of *VirnetX Inc. v. Microsoft Corporation*, the Patent Owner accused Microsoft of infringing the ’180 patent by asserting that a 32-character hexadecimal string— invisible to the user—was a “secure domain name”:

Q. Can you -- you say that there's a secure group name that's used to find the group. Can you give us an example of what the secure group name looks like?

A. Sure. The secure group name -- one example of this is given on this slide. This is *a long string of characters* on the left side followed by a dot and then a classifier associated with an application.⁵

* * *

Q. Okay. Well, Professor Jones, though, are you calling a secure group name a secure domain name for purposes of these patents just because they both say the word secure?

A. No. I'm not calling it just because they use that name secure. I analyzed these and matched them to the claim elements rather than just say, well, they say it's a secure name, so it must meet the claim terms.

⁴ Reexamination Control No. 95/001,270, Action Closing Prosecution at 3 (Jun. 16, 2010).

⁵ Ex. 1, *VirnetX v. Microsoft*, No. 6:07-cv-80 (E.D. Tex.), Trial Transcript, testimony of VirnetX expert witness Mark Jones, at 158-59 (Day 2 Afternoon, Mar. 9, 2010).

Q. So why does the secure group name look like that, *all that crazy chaos, the 5fe531661*, et cetera?

A. Well, it looks like that so that you can have some assurance that it's the right name. They use that kind of name, because it's difficult to fake that name. It's hard for someone -- or almost impossible for someone to fake the correct secure group name.⁶

* * *

A. This is deposition testimony, sworn testimony from Mr. Christian Huitema. He was asked: Can you tell by looking at a secure peer name, that it must be resolved by PNRP rather than DNS?

His answer: Oh, yes. They have a very different syntax, APN. A DNS name will be something like *www.microsoft.com*, whereas a peer name, a secure peer name, in particular, will include a sequence of *32 hexadecimal digits*.

Q. Well, so we've got a crazy secure group name. How can the PeerNet interfaces in the Windows I'm running -- and I'm assuming *the user doesn't have to deal with that crazy name*, correct?

A. That's correct.⁷

The Patent Owner won on this infringement theory, and Microsoft subsequently paid \$200 million for a license covering the '180 patent.⁸

⁶ Ex. 1, *VirnetX v. Microsoft*, No. 6:07-cv-80 (E.D. Tex.), Trial Transcript, testimony of VirnetX expert witness Mark Jones, at 160 (Day 2 Afternoon, Mar. 9, 2010).

⁷ Ex. 1, *VirnetX v. Microsoft*, No. 6:07-cv-80 (E.D. Tex.), Trial Transcript, testimony of VirnetX expert witness Mark Jones, at 160 (Day 2 Afternoon, Mar. 9, 2010).

⁸ Press Release, Microsoft and VirnetX Settle Patent Infringement Cases (May 17, 2010), available at <http://www.microsoft.com/presspass/press/2010/may10/05-17newspr.msp>.

In the currently-pending litigation, the Patent Owner's infringement contentions assert that an IP address (such as "10.0.0.12") or a telephone number is a "secure domain name":

Further, a secure domain name service is provided, for example, by the NHRP server. The NHRP [Next Hop Resolution Protocol] server responds to queries from spokes requesting the address of destinations behind other spokes. Page 3 of Attachment C-28 [of the infringement contentions] states, for example, "*Spoke A consults its NHRP mapping table for destination 10.0.0.12 and does not find an entry. So it sends an NHRP query packet to the NHRP server.*"

A secure domain name is, for example, an internal address of a resource on a spoke subnetwork or the tunnel address of the spoke associated with a particular resource. For example, a secure domain could be the internal address of a web server behind a particular spoke (spoke B) or the tunnel address of spoke B.

* * *

A secure domain name service is provided, for example, by the IME validation process described in the [infringement contentions]. *The IME validation process attempts to resolve a particular number to its associated SIP URI.* This is shown, for example, at pages 3-5 of Attachment C-29 [to the infringement contentions]. *A secure domain name can, for example, be a number associated with the called IP phone* or other SIP endpoint within the IME system.⁹

⁹ Ex. 2, Letter from Ramzi Khazen, counsel for VirnetX, to Dmitriy Kheyfits, counsel for Cisco (June 23, 2011), Attachment A at 7 (attempting to clarify VirnetX's infringement contentions).

Thus, the Patent Owner asserts that *anything except* a conventional domain name is a “secure domain name.” As explained in greater detail below, the Examiner did not consider these issues in deciding not to order reexamination.

B. Lendenmann Teaches Resolving “Secure Domain Names”

As detailed in the Request, Lendenmann teaches a name service capable of resolving both conventional domain names and CCITT X.500 names. The Request asserts that Lendenmann’s disclosure of an X.500 name teaches the asserted claim limitation of a “secure domain name.”

The examiner provided two reasons for denying the Request. First,

- 1) a name provided, i.e. the conventions and syntax requirements thereof, which enforces/reflects the CCITT X.500 naming scheme will not be resolved by the DNS server regardless of whether it is a secure/non-standard domain name or non-secure/standard domain name because the CCITT X.500 naming scheme is incompatible with/mutually exclusive of the DNS naming scheme.¹⁰

In essence, the examiner states that the X.500 naming scheme is wholly separate and different from the conventional DNS naming scheme, and therefore an X.500 name cannot be considered a “domain name,” let alone a “secure domain name.” The examiner’s statements, however, fail to appreciate the Patent Owner’s assertion that *anything except* a conventional domain name is a “secure domain name.” Thus, the fact that the X.500 naming scheme is mutually incompatible with the conventional DNS naming scheme is actually evidence—under the Patent Owner’s interpretation—that Lendenmann teaches the “secure domain name” limitation. An X.500 name is *necessarily* not a conventional domain name.

And the examiner’s statement that an X.500 name “will not be resolved by the DNS server” further establishes a reasonable likelihood that the Requester will prevail. As the Patent Owner asserted in the previous reexamination, the hallmark of a “secure domain name” is that it

¹⁰ Order Denying Request for *Inter Partes* Reexamination at 4 (Dec. 17, 2011).

“cannot be resolved by a conventional domain name service.” Thus, the fact that a conventional DNS server will not resolve the X.500 name shows that Lendenmann’s X.500 names are “secure domain names” under the Patent Owner’s claim interpretation.

As a second reason for denying the Request, the examiner stated:

2) the name service of DCE resolves names regardless of whether a name provided, i.e. conventions and syntax requirements thereof, enforces/reflects the CCITT X.500 or DNS or CDS naming scheme....¹¹

As explained in the Request, Lendenmann teaches a name server that is capable of resolving *both* conventional DNS *and* CCITT X.500 names.

The examiner’s statement suggests that Lendenmann’s name server cannot be a “secure domain name service” because it is capable of resolving both “secure” and conventional domain names. But this statement confuses the Patent Owner’s definition-by-subtraction of this claim term. The Patent Owner asserts that “a conventional domain name service cannot resolve addresses for a secure domain name.”¹² But the Patent Owner has not suggested imposing a converse requirement that a “secure domain name service” be unable to resolve a *conventional* domain name. Thus, the presence of additional functionality in Lendenmann’s name server—namely, the ability to resolve *conventional* domain names—does not interfere with Lendenmann’s clear teaching of a server that can resolve a “secure domain name.”

In summary, the examiner’s statements regarding Lendenmann actually increase the likelihood that Requester will prevail with respect to claims in the ‘180 patent under the Patent Owner’s interpretation. On *de novo* review of these issues, the Director should order reexamination of claims 1-41 of the ‘180 patent.

¹¹ Order Denying Request for *Inter Partes* Reexamination at 4 (Dec. 17, 2011).

¹² Reexamination Control No. 95/001,270, Action Closing Prosecution at 3 (Jun. 16, 2010).

C. Kiuchi Teaches Resolving “Secure Domain Names”

The Request explained in detail Kiuchi’s secure C-HTTP naming scheme. The examiner provided two reasons for denying the Request. First,

1) a host name, while not necessarily having to be the same as its DNS name, although it could be, is also not disclosed as being “a non-standard domain name”, e.g. it could be a standard name with appropriate certification¹³

Thus, the examiner understood Kiuchi as teaching that a computer’s C-HTTP name may be different from its conventional DNS name.¹⁴ But the examiner apparently failed to appreciate that if the C-HTTP name is different, then a conventional DNS service will be unable to resolve the C-HTTP name.

And the examiner apparently overlooked Kiuchi’s example C-HTTP names, which are plainly “non-standard” domain names. Specifically, Kiuchi provides two example names: “Coordinating.Center.CSCRG” and “University.of.Tokyo.Branch.Hospital”.¹⁵ The Request specifically identified the first of these as the claimed “secure domain name”.¹⁶

As shown in Kiuchi Appendix 3, the secure server-side proxy is identified by the secure domain name, i.e. “hostname,”
“Coordinating.Center.CSCRG.”

As a second reason for denying the Request, the examiner stated:

nor 2) is the querying of the name server using such name disclosed as resulting in a return message indicating that the URL

¹³ Order Denying Request for *Inter Partes* Reexamination at 9 (Dec. 17, 2011).

¹⁴ *See, e.g.*, Kiuchi at 68 (“As C-HTTP includes its own secure name service, which contains a certification mechanism, it is impossible to know the IP address of a server-side proxy even if its C-HTTP hostname (not necessarily the same as its DNS name) is known and vice versa.”).

¹⁵ Kiuchi at 73.

¹⁶ Request for Reexamination, Ex. E-2 at 6.

is "unknown", see, e.g., page 68, col. 1, section 2) and Appendix 2, section 1.2 of Kiuchi, e.g. return message is "OK" or "Disallowed", i.e. the latter does not disclose names are "unknown" as compared to, e.g., "uncertified". In other words, Kiuchi requires a host name which is associated with a secure computer, i.e. simultaneous hostname resolution and host certification.¹⁷

But to the extent that the examiner believes that a "secure domain name service" must return the error message "unknown" when presented with a "secure domain name," the examiner fundamentally misunderstands and misapplies the Patent Owner's interpretative statements from the first reexamination. It is a *conventional* domain name service that provides an "unknown" response when presented with a "secure domain name." Kiuchi's C-HTTP name server is identified as the "secure domain name service":¹⁸

For these reasons, the C-HTTP name server is a "secure domain name service," as recited in the claim.

Therefore the C-HTTP name server *should* be able to resolve a "secure domain name." The examiner's expectation that it should return an "Unknown" message is simply wrong.

In summary, the examiner's statements regarding Kiuchi misapply the asserted interpretations of a "secure domain name" and a "secure domain name service." When the Patent Owner's interpretation is correctly applied, Kiuchi establishes a reasonable likelihood that the Requester will prevail with respect to claims 1-41 of the '180 patent. The Director should order reexamination of these claims.

D. Solana

Regarding the Solana reference, the examiner found that Solana taught an X.509 system rather than the claimed secure domain name system:

¹⁷ Order Denying Request for *Inter Partes* Reexamination at 9 (Dec. 17, 2011).

¹⁸ Request for Reexamination, Ex. E-2 at 9-10.

Solana discloses X.509 is a protocol which proposes a standardized method to store certificates in a world-wide distributed data base which associates end-users to their public key, regardless of whether a user's name is a standard or non-standard domain name, i.e. the name with respect to its conventions and syntax thereof. Solana does not disclose X.509 provides a non-standard domain name which can not be resolved by a conventional domain name service and results in a return message URL "unknown" but rather digital certification authenticating the user of a name, see, e.g., pages 29 and 43 thereof.¹⁹

First, Requester notes that even if much of Solana's disclosure focuses on additional features not recited in the claims, Solana nevertheless discloses the claimed technology. As the examiner acknowledges, Solana's X.509 service does not require a user's name to be a standard domain name. And as the Requester explained, Solana provides examples of names that are not conventional domain names and that could not be resolved by a conventional domain name service.²⁰ Requester again notes that the Patent Owner asserts that *any name other than a conventional domain name* is a "secure domain name," regardless of whether the name complies with some other naming syntax or convention.

On *de novo* review of Solana in view of the Patent Owner's interpretation of the claims, the Director should order reexamination of the '180 patent.

E. Schimpf and Rosenberry

Regarding the combination of Schimpf and Rosenberry, the examiner found that these references "do not teach a 'secure domain name' and a 'secure domain name service' as set forth in the claims."²¹ The examiner provided two reasons for reaching this conclusion:

¹⁹ Order Denying Request for *Inter Partes* Reexamination at 14 (Dec. 17, 2011).

²⁰ See Request for Reexamination, Ex. E-3 at 4 (noting how "information may be stored in an 'X.509' infrastructure," which Solana distinguishes from a DNS infrastructure).

²¹ Order Denying Request for *Inter Partes* Reexamination at 15 (Dec. 17, 2011).

1) a name provided, i.e. the conventions and syntax requirements thereof, which enforces/reflects the respective naming scheme/component, e.g. the CDS, X.500 or DNS scheme/component, will not be resolved by a server of another naming scheme component, e.g., DNS and/or X.500, regardless of whether it is a secure/non-standard domain name or non-secure/standard domain name because the naming scheme is incompatible with/mutually exclusive of the other components' naming schemes²²

This explanation is substantially the same as that given regarding Lendenmann. As explained above, the fact that X.500 names are mutually exclusive of conventional domain names shows that an X.500 name is a “secure domain name” under the Patent Owner’s interpretation. Thus, Schimpf and Rosenberry teach the claimed “secure domain name” and “secure domain name service.”

As a second reason, the examiner stated:

2) the name service of DCE resolves names regardless of whether a name provided, i.e. conventions and syntax requirements thereof, enforce/reflect any of the naming schemes.²³

This statement is again similar to that given regarding Lendenmann. And as explained above, the ability of the Schimpf/Rosenberry name service to resolve conventional domain names does not negate its status as a “secure domain name service.” The Patent Owner asserts that the only requirement of a “secure domain name service” is that it be able to resolve a “secure domain name”—that is, be able to resolve a name which is not a conventional domain name. Thus, under the Patent Owner’s claim interpretation, Schimpf and Rosenberry teach the critical limitations. On *de novo* review, Requester respectfully requests that the Director order reexamination of the ’180 patent.

²² Order Denying Request for *Inter Partes* Reexamination at 15 (Dec. 17, 2011).

²³ Order Denying Request for *Inter Partes* Reexamination at 15-16 (Dec. 17, 2011).

VI. Actions Requested

Based on the foregoing, Requester hereby respectfully requests the Director to order reexamination of claims 1-41 of the '180 patent.

VII. Conclusion

The decision denying the Request to reexamine the '180 patent failed to properly consider the Patent Owner's claim interpretation. As discussed above, the references explicitly disclose all of the limitations stated to be missing in the Order. Requester respectfully requests that the Director order reexamination of the '180 Patent.

In accordance with 37 C.F.R. § 1.17(f), this request is accompanied by a credit card authorization for payment of the fee of \$400.00. The Commissioner is hereby authorized to charge any deficiency or credit any overpayment for this request to Deposit Account No. 08-1394.

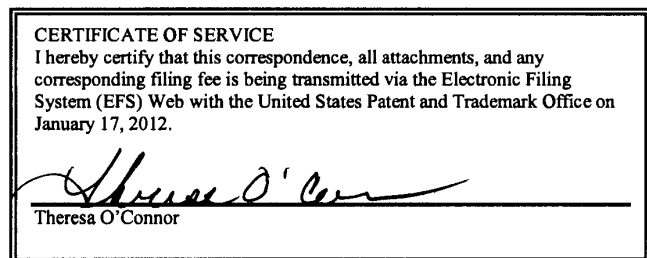
As identified in the attached Certificate of Service, a copy of the present petition, in its entirety, is being served to the address of the attorney or agent of record.

Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: January 17, 2012
HAYNES AND BOONE, LLP
IP Section, 2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Facsimile: 214/200-0853
R295245.1



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Reexamination Control No.: 95/001,792	§	Attorney Docket No.: 43614.100
	§	
Patent No.: 7,188,180	§	Customer No.: 27683
	§	
For: METHOD FOR ESTABLISHING	§	Real Party In Interest:
SECURE COMMUNICATION LINK	§	Cisco Systems, Inc.
BETWEEN COMPUTERS OF	§	
VIRTUAL PRIVATE NETWORK	§	
	§	
Examiner: Karin M. Reichle	§	
	§	
Art Unit: 3992	§	Conf. No. 1972

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

CERTIFICATE OF SERVICE

Pursuant to M.P.E.P. § 2266.06 and 37 C.F.R. §§ 1.248 and 1.903, the undersigned attorney for the Third Party Requester certifies that a copy of the PETITION UNDER 37 C.F.R. §§ 1.927 and 1.181 and Exhibits 1-2 was served on January 17, 2012 on the counsel for Patent Owner at the following address:

McDermott Will & Emery
600 13th Street, NW
Washington DC 20005-309

In addition, it is noted that the Patent Owner has filed a Power of Attorney purportedly to change the attorney of record for this reexamination proceeding only (without changing the attorney of record for the underlying patent, in contravention of 37 U.S.C. § 1.33(c) and MPEP § 2622). Accordingly, on January 17, 2012, a courtesy copy of the PETITION UNDER 37 C.F.R. §§ 1.927 and 1.181 and Exhibits 1-2 was served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

/David L. McCombs/

David L. McCombs, Reg. No. 32,271

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:	11847668
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	17-JAN-2012
Filing Date:	25-OCT-2011
Time Stamp:	13:01:02
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$400
RAM confirmation Number	15946
Deposit Account	081394
Authorized User	MCCOMBS,DAVID L

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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Petition_For_Reconsideration.pdf	818667 78b42da6ace24087e8da37b1fe6348a081db077	yes	15
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Receipt of Petition in a Reexam	1	14	
		Reexam Certificate of Service	15	15	
Warnings:					
Information:					
2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex1_Trial_Transcript_Mark_Jones.pdf	229149 caf0154819b5a0ac584700da27b0c31ab1e2e3be	no	7
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex2_Letter_From_Counsel_For_Virnetx.pdf	974716 0c0e9eb68b3b5523fa3e6230cf1c8ac852ddf0aa0	no	13
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30698 2105752f93ce6f4b46fbc67da4ae569dccc61387	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2053230		

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.
-----------------	-------------	----------------------	---------------------	------------------

95/001,792	10/25/2011	7,188,180	43614.100	1972
------------	------------	-----------	-----------	------

22852 7590 12/17/2011
 FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
 LLP
 901 NEW YORK AVENUE, NW
 WASHINGTON, DC 20001-4413

EXAMINER

REICHLER, KARIN M

ART UNIT	PAPER NUMBER
----------	--------------

3992

MAIL DATE	DELIVERY MODE
-----------	---------------

12/17/2011

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

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Date: 12-17-11

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001792
PATENT NO. : 7188180
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)

Transmittal of Communication to Third Party Requester Inter Partes Reexamination	Control No.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	KARIN REICHLE	3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

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.	Patent Under Reexamination
	95/001,792	7,188,180
	Examiner	Art Unit
	KARIN REICHLE	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 does not establish a reasonable likelihood that requester will prevail with respect to claims 1-41 of United States Patent Number 7,188,180 (Larson et al)

References Cited in Request

A total of ten references, alone or in certain combinations, have been asserted in the Request as providing teachings relevant to the claims of the Larson et al '180 patent. The references are as follows:

Rolf Lendenmann, UNDERSTANDING OSF DCE 1.1 FOR AIX AND OS/2, IBM International Technical Support Organization (Oct. 1995) (hereinafter referred to as Lendenmann).

Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet," published in the Proceedings of SNDSS 1996 (hereinafter referred to as Kiuchi).

Eduardo Solana and Jurgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains," Security Protocols Workshop 1997, pp. 37-51 (hereinafter referred to as Solana).

David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998) (hereinafter referred to as Martin).

Bruce Schneier, APPLIED CRYPTOGRAPHY (1996) (hereinafter referred to as Schneier).

Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Protocol Specification RFC 793 (Sept. 1981) (hereinafter referred to as RFC 793).

Brian C. Schimpf, "Securing Web Access with DCE," presented at Network and Distributed System Security (Feb. 10-11, 1997) (hereinafter referred to as Schimpf).

Art Unit: 3992

Ward Rosenberry, David Kenney, and Gerry Fisher, UNDERSTANDING DCE (1993) (hereinafter referred to as Rosenberry).

Daniel R. Masys & Dixie B. Baker, "Protecting Clinical Data on Web Client Computers: the PCASSO Approach," Proceedings of the AMIA'98 Annual Symposium, Orlando, FL (Nov. 7-11, 1998) (hereinafter referred to as Masys).

"Domain Names- Concepts and Facilities," RFC 1034 (Nov., 1987) (hereinafter referred to as RFC 1034).

Identification of Every Claim for Which Reexamination is Requested

The ten references cited above are discussed in the Request and asserted to render unpatentable claims 1-41 of the Larson et al '180 patent. Pages 3-24 and Exhibits E1-E4 of the Request include explanations that seek to establish a reasonable likelihood that the requester will prevail with respect to at least one of the patent claims in light of the ten references cited above. The explanations in the Request are addressed below under subheadings designating each one as a numbered "Issue".

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

Lendenmann
(referencing RFC 793 and RFC 1034)

The proposed rejection of claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 as set forth at pages 3, 12-15 and 21-23 of the Request and pages 2-67 of the Claim Chart, Exhibit E-1, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. Lendenmann, however, does not teach a “secure domain name” and a “secure domain name service” as set forth in such claims. See the prosecution history with regard to the interpretation of such claim language, e.g., the paragraph bridging pages 10-11 of the Request and pages 13-14 of the 6-16-10 Action Closing Prosecution of the first reexam, Reexamination Control No. 95/001270, of the Larson ‘180 patent. Contrary to the Request at pages 12-15 and pages 2-67 of the Claim Chart, Exhibit E-1, the CCITT X.500 naming scheme of the name service of the Distributed Computing environment (DCE) of Lendenmann does not provide a “secure domain name” and a “secure domain name service” as so interpreted, e.g. 1) a name provided, i.e. the conventions and syntax requirements thereof, which enforces/reflects the CCITT X.500 naming scheme will not be resolved by the DNS server regardless of whether it is a secure/non-standard domain name or non-secure/standard domain name because the CCITT X.500 naming scheme is incompatible with/mutually exclusive of the DNS naming scheme and 2) the name service of DCE resolves names regardless of whether a name provided, i.e. conventions and syntax requirements thereof, enforces/reflects the CCITT X.500 or DNS or CDS naming scheme, see, e.g., Section 1.4.4 on page 10 and sections 2.2-2.3.6 on pages 21-28 of Lendenmann (also note the discussion of DCE in Rosenberry at, e.g., pages 30-37, 160 and 213 as well as the discussion

Art Unit: 3992

thereof in Issue 10, *infra*). For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 as set forth at pages 3, 12-15 and 21-23 of the Request and pages 2-67 of the Claim Chart, Exhibit E-1, which are incorporated by reference, since it is deemed that Lendenmann does not teach the missing limitations as noted with regards to 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 above.

Therefore, it is not found that the consideration of Lendenmann establishes that there is a reasonable likelihood that the requester will prevail with respect to 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40.

Issue 2

Lendenmann and Schneier

The proposed rejection of dependent claims 5, 21 and 36 as set forth at pages 3, 12-15 and 21-23 of the Request and pages 68-72 of the Claim Chart, Exhibit E-1, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. The requester provides prior art to Schneier for the teaching of encrypting by inserting one or more data values which vary according to a pseudo-random sequence. Therefore Lendenmann or Schneier cannot be utilized alone or combined to teach a "secure domain name" and a "secure domain name service" as set forth in claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 from which claims 5, 21 and 36 depend, see, e.g., Claim Chart mapping, sections [5.0], [21.0] and [36.0], and the discussion of claim interpretation in Issue 1 *supra*. In addition, the Request states "[a]nd as analyzed above

Art Unit: 3992

in portions [1.0] and [6.1], Lendenmann teaches encrypting data packets using the DSE encryption standard.” However the terminology “DSE” never even appears in such analysis and thereby, the Claim Chart mapping, e.g., sections [5.1], [21.1 and [36.1], is not clear. For the reasons above, the Request does not establish that there is a reasonable likelihood of success with respect to claims 5, 21 and 36 as asserted by the third party requester in the Request for reexamination.

Therefore, it is not found that the consideration of Lendenmann and Schneier establishes that there is a reasonable likelihood that the requester will prevail with respect to claims 5, 21 and 36.

Issue 3

Lendenmann and Martin

The proposed rejection of dependent claims 7, 23 and 38 as set forth at pages 3, 12-15 and 21-23 of the Request and pages 73-76 of the Claim Chart, Exhibit E-1, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. The requester provides prior art to Martin for the teaching of establishing a virtual private network communication link by creating a network address hopping regime between a first computer and a second computer. Therefore Lendenmann or Martin cannot be utilized alone or combined to teach a “secure domain name” and a “secure domain name service” as set forth in claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 from which claims 7, 23 and 38 depend, see, e.g., Claim Chart mapping, sections [7.0], [23.0] and [38.0], and the discussion of claim interpretation

in Issue 1 supra. In addition, the Request states “[o]ne of skill in the art would have been motivated to combine Martin's IP hopping scheme with Lendenmann's secure remote procedure call in order to obfuscate a client computer's network location, as described in Martin.” However the “Lendenmann's secure remote procedure call” is not discussed and thereby, the Claim Chart mapping, e.g., sections [7.1], [23.1] and [38.1], is not clear. For the reasons above, the Request does not establish that there is a reasonable likelihood of success with respect to claims 7, 23 and 38 as asserted by the third party requester in the Request for reexamination.

Therefore, it is not found that the consideration of Lendenmann and Martin establishes that there is a reasonable likelihood that the requester will prevail with respect to claims 7, 23 and 38.

Issue 4

Lendenmann

The proposed rejection of dependent claims 11, 27 and 41 as set forth at pages 3, 12-15 and 21-23 of the Request and pages 77-78 of the Claim Chart, Exhibit E-1, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. However, as discussed supra, Lendenmann does not teach a “secure domain name” and a “secure domain name service” as set forth in claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 from which claims 11, 27 and 41 depend, see, e.g., Claim Chart mapping, sections [11.0], [27.0] and [41.0], and the discussion of claim interpretation in Issue 1 supra. In addition, the Request states “[i]n view of Lendenmann' s disclosure of a secure domain name (portion [1.1]) that is different

Art Unit: 3992

from a conventional DNS name (portion [2.1b]), a person of ordinary skill in the art would have considered the use of a top level domain name that includes .scorn, .snet, .sorg, .sedu, .smil, or .sgov to be a matter of mere design choice. Design choice is ‘an acceptable rationale for an obviousness rejection when a claimed product merely arranges known elements in a configuration recognized as functionally equivalent to a known configuration.’ See, Ex parte Gunasekar, Appeal 2009-008345 in 10/903,590 (BPAI 2011). *Since* Lendenmann teaches secure domain names that correspond to conventional domain names and since .com, .net, .org, .edu, and .gov are character combinations commonly known to represent top level domain names, arranging the known top level domain name character combinations with the additional known character "s" to abbreviate the descriptive term "security" is an obvious design choice.”

(Emphasis added.) However, the addition of characters is not mere rearrangement of the known elements nor is the disclosure of a different name the teaching of a corresponding name and thereby, the Claim Chart mapping, e.g., sections [11.1], [27.1] and [41.1], is not clear and does not provide a proper rationale to support a conclusion of obviousness. For the reasons above, the Request does not establish that there is a reasonable likelihood of success with respect to claims 11, 27 and 41 as asserted by the third party requester in the Request for reexamination.

Therefore, it is not found that the consideration of Lendenmann establishes that there is a reasonable likelihood that the requester will prevail with respect to claims 11, 27 and 41.

Issue 5

Kiuchi
(referencing RFC 793)

The proposed rejection of claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 as set forth at pages 3-4, 15-17, and 21-23 of the Request and pages 2-42 of the Claim Chart, Exhibit E-2, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. *Kiuchi*, however, does not teach a “secure domain name” and a “secure domain name service” as set forth in such claims. See the prosecution history with regard to the interpretation of such claim language, e.g., the paragraph bridging pages 10-11 of the Request and pages 13-14 of the 6-16-10 Action Closing Prosecution of the first reexam, Reexamination Control No. 95/001270, of the Larson ‘180 patent. Contrary to the Request at pages 15-17 and pages 2-42 of the Claim Chart, Exhibit E-2, the C-HTTP naming scheme of *Kiuchi* does not provide a “secure domain name” and a “secure domain name service” as so interpreted, e.g. 1) a host name, while not necessarily having to be the same as its DNS name, although it could be, is also not disclosed as being “a non-standard domain name”, e.g. it could be a standard name with appropriate certification, nor 2) is the querying of the name server using such name disclosed as resulting in a return message indicating that the URL is “unknown”, see, e.g., page 68, col. 1, section 2) and Appendix 2, section 1.2 of *Kiuchi*, e.g. return message is “OK” or “Disallowed”, i.e. the latter does not disclose names are “unknown” as compared to, e.g., “uncertified”. In other words, *Kiuchi* requires a host name which is associated with a secure computer, i.e. simultaneous host name resolution and host certification. For the reasons above, the Request does not establish that there is a reasonable likelihood that the requester will prevail with regard to claims 1-2, 4-6, 8-

Art Unit: 3992

10, 12-18, 20-22, 24-26, 28-37, and 39-40 as set forth at pages 3-4, 15-17, and 21-23 of the Request and pages 2-42 of the Claim Chart, Exhibit E-2, which is incorporated by reference, since it is deemed that Kiuchi does not teach the missing limitations as noted with regards to 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 above.

Therefore, it is not found that the consideration of Kiuchi establishes that there is a reasonable likelihood that the requester will prevail with respect to 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40.

Issue 6

Kiuchi and Masys

The proposed rejection of dependent claims 3 and 19 as set forth at pages 3-4, 15-17, and 21-23 of the Request and pages 43-46 of the Claim Chart, Exhibit E-2, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. The requester provides prior art to Masys for the teaching of running a Patient Centered Access to Secure Systems Online (PCASSO) program by selecting an icon to run a Supplemental Protection for the Client Environment (SPICE) program. Therefore Kiuchi or Masys cannot be utilized alone or combined to teach a “secure domain name” and a “secure domain name service” as set forth in claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 from which claims 3 and 19 depend, see, e.g., Claim Chart mapping, sections [3.0], and [19.0], and the discussion of claim interpretation in Issue 5 supra. In addition, it is not clear, via the Claim Chart mapping (pages 43-46), how exactly the teachings of pages 44-46, i.e. sections [3.1] and [19.1], “render obvious”

Art Unit: 3992

the claim limitations as well as what the specific basis, e.g., which portions of Kiuchi and Masys, support the reasons/conclusions set forth on page 43 of the Request. For the reasons above, the Request does not establish that there is a reasonable likelihood of success with respect to claims 3 and 19 as asserted by the third party requester in the Request for reexamination.

Therefore, it is not found that the consideration of Kiuchi and Masys establishes that there is a reasonable likelihood that the requester will prevail with respect to claims 3 and 19.

Issue 7

Kiuchi and Martin

The proposed rejection of dependent claims 7, 23 and 38 as set forth in pages 3, 15-17, and 21-23 of the Request and pages 47-50 of the Claim Chart, Exhibit E-2, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. The requester provides prior art to Martin for the teaching of establishing a virtual private network communication link by creating a network address hopping regime between a first computer and a second computer. Therefore Kiuchi or Martin cannot be utilized alone or combined to teach a “secure domain name” and a “secure domain name service” as set forth in claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 from which claims 7, 23 and 38 depend, see, e.g., Claim Chart mapping, sections [7.0], [23.0] and [38.0], and the discussion of claim interpretation in Issue 5 supra. In addition, the Request states “[o]ne of skill in the art would have been motivated to combine Martin's IP hopping scheme with Kiuchi's secure, closed network in order to further provide anonymity protection to the network participants, as described in Martin.” However

Art Unit: 3992

“Kiuchi’s secure, closed network”, e.g. such desiring anonymity protection to the network participants, is not discussed and thereby, the Claim Chart mapping, e.g., sections [7.1], [23.1] and [38.1], is not clear. For the reasons above, the Request does not establish that there is a reasonable likelihood of success with respect to claims 7, 23 and 38 as asserted by the third party requester in the Request for reexamination.

Therefore, it is not found that the consideration of Kiuchi and Martin establishes that there is a reasonable likelihood that the requester will prevail with respect to claims 7, 23 and 38.

Issue 8

Kiuchi

The proposed rejection of dependent claims 11, 27 and 41 as set forth at pages in 3, 15-17, and 21-23 and of the Request and pages 51-52 of the Claim Chart, Exhibit E-2, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. However, as discussed supra, Kiuchi does not teach a “secure domain name” and a “secure domain name service” as set forth in claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 from which claims 11, 27 and 41 depend, see, e.g., Claim Chart mapping, sections [11.0], [27.0] and [41.0], and the discussion of claim interpretation in Issue 5 supra. In addition, the Request states “[i]n view of Kiuchi’s disclosure of a secure domain name (portion [1.1]) that is different from a conventional DNS name (portion [2.1b]), a person of ordinary skill in the art would have considered the use of a top level domain name that includes .scorn, .snet, .sorg, .sedu, .smil, or .sgov to be a matter of mere design choice. Design choice is ‘an acceptable rationale for an

Art Unit: 3992

obviousness rejection when a claimed product merely arranges known elements in a configuration recognized as functionally equivalent to a known configuration.' See, Ex parte Gunasekar, Appeal 2009-008345 in 10/903,590 (BPAI 2011). *Since* Kiuchi teaches secure domain names that correspond to conventional domain names and since .com, .net, .org, .edu, and .gov are character combinations commonly known to represent top level domain names, arranging the known top level domain name character combinations with the additional known character "s" to abbreviate the descriptive term "security" is an obvious design choice."

(Emphasis added.) However, the addition of characters is not mere rearrangement of the known elements nor is the disclosure of a different name the teaching of a corresponding name and thereby, the Claim Chart mapping, e.g., sections [11.1], [27.1] and [41.1], is not clear and does not provide a proper rationale to support a conclusion of obviousness. For the reasons above, the Request does not establish that there is a reasonable likelihood of success with respect to claims 11, 27 and 41 as asserted by the third party requester in the Request for reexamination.

Therefore, it is not found that the consideration of Kiuchi establishes that there is a reasonable likelihood that the requester will prevail with respect to claims 11, 27 and 41.

Issue 9

Solana

The proposed rejection of claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33 and 35 as set forth at pages 4, 17-19 and 24 of the Request and pages 2-17 of the Claim Chart, Exhibit E-3, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. Solana,

Art Unit: 3992

however, does not teach a “secure domain name” and a “secure domain name service” as set forth in such claims. See the prosecution history with regard to the interpretation of such claim language, e.g., the paragraph bridging pages 10-11 of the Request and pages 13-14 of the 6-16-10 Action Closing Prosecution of the first reexam, Reexamination Control No. 95/001270, of the Larson ‘180 patent. Contrary to the Request at pages 17-19 and pages 2-17 of the Claim Chart, Exhibit E-2, Solana discloses X.509 is a protocol which proposes a standardized method to store certificates in a world-wide distributed data base which associates end-users to their public key, regardless of whether a user’s name is a standard or non-standard domain name, i.e. the name with respect to its conventions and syntax thereof. Solana does not disclose X.509 provides a non-standard domain name which can not be resolved by a conventional domain name service and results in a return message URL “unknown” but rather digital certification authenticating the user of a name, see, e.g., pages 29 and 43 thereof. 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, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33 and 35, as set forth at pages 4, 17-19 and 24 of the Request and pages 2-17 of the Claim Chart, Exhibit E-3, which are incorporated by reference, since it is deemed that Solana does not teach the missing limitations as noted with regards to 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33 and 35, above.

Therefore, it is not found that the consideration of Solana establishes that there is a reasonable likelihood that the requester will prevail with respect to 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33 and 35.

Issue 10

Schimpf and Rosenberry

The proposed rejection of claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 as set forth at pages 3-4, 19-20, 21 and 24 of the Request and pages 2-19 of the Claim Chart, Exhibit E-4, which are incorporated by reference, is relied upon in the Request to show a reasonable likelihood that the requester will prevail with respect to at least one of the claims of the patent. The requester provides prior art to Schimpf for the teaching a naming scheme, CDS, of a name service of a Distributed Computing Environment (DCE) and to Rosenberry for teaching examples of DCE names. Schimpf and Rosenberry, however, do not teach a “secure domain name” and a “secure domain name service” as set forth in the claims. See the prosecution history with regard to the interpretation of such claim language, e.g., the paragraph bridging pages 10-11 of the Request and pages 13-14 of the 6-16-10 Action Closing Prosecution of the first reexam, Reexamination Control No. 95/001270, of the Larson ‘180 patent. Contrary to the Request at pages 19-20 and pages 2-19 of the Claim Chart, Exhibit E-4, the naming schemes/components of the name service of the Distributed Computing Environment (DCE) of Schimpf and Rosenberry do not provide a “secure domain name” and a “secure domain name service” as so interpreted, e.g. 1) a name provided, i.e. the conventions and syntax requirements thereof, which enforces/reflects the respective naming scheme/component, e.g. the CDS, X.500 or DNS scheme/component, will not be resolved by a server of another naming scheme component, e.g., DNS and/or X.500, regardless of whether it is a secure/non-standard domain name or non-secure/standard domain name because the naming scheme is incompatible with/mutually exclusive of the other components’ naming schemes and 2) the name service of DCE resolves

Art Unit: 3992

names regardless of whether a name provided, i.e. conventions and syntax requirements thereof, enforce/reflect any of the naming schemes, see, e.g., Rosenberry also at pages 30-37, 160 and 213 (note also the discussion of DCE in Section 1.4.4 on page 10 and sections 2.2-2.3.6 on pages 21-28 of Lendenmann, esp. 2.3.6 with regard to the CDS naming scheme, as well as the discussion thereof in Issue 1 supra). 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, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 as set forth 3-4, 19-20, 21 and 24 of the Request and pages 2-19 of the Claim Chart, Exhibit E-4, which are incorporated by reference, since it is deemed that Schimpf and Rosenberry do not teach the missing limitations as noted with regards to 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35 above.

Therefore, it is not found that the consideration of Schimpf and Rosenberry establish that there is a reasonable likelihood that the requester will prevail with respect to 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, and 35.

Summary

Claims 1-41 of the Larson et al '180 patent will not be reexamined as requested in the Order.

Other Matters

Availability of Asserted References as Prior Art

The earliest effective filing date of claims 1-41 of the Larson '180 patent is considered to be April 26, 2000.

Art Unit: 3992

With regard to the request set forth in section II, B. of the 11-17-11 Patent Owner Petition, see prosecution history of the instant re-examination, e.g., the 12-1-11 Requester Petition and accompanying exhibits.

Therefore, the references to Lendenmann, Kiuchi, Solana, Schneier, RFC 793, Schimpf, Rosenberry Masys and RFC 1034 are “printed” and “published” at least more than one year prior to the effective filing date of April 26, 2000 of the claims of the ‘180 patent and thus are available as prior art under 35 USC 102(b) and 35 USC 103.

The reference to Martin is printed and “published” at least prior to the effective filing date of April 26, 2000 of the claims of the ‘180 patent and thus is available as prior art under 35 USC 102(a) and 35 USC 103.

Conclusion

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
 Attn: Central Reexamination Unit
 Commissioner of 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 St.
 Alexandria, VA 22314

By EFS-Web:

Art Unit: 3992

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 examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Conferees:

/Karin M. Reichle/
Primary Examiner, Art Unit 3992

/ALN/

Matthew L. Brooks
Matthew L. Brooks
SPE CRU 3992-AU

Receipt date: 10/25/2011

95001792 - GAU: 3992

In place of PTO-1449 Form		U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Application Number	<i>Inter Partes</i> Reexamination of U.S. Patent No. 7,188,180
				Filing Date	October 25, 2011
				Real Parties in Interest	Cisco Systems, Inc.
				Art Unit	788 3392
				Examiner Name	TBD Reichle
SHEET	1	OF	1	Attorney Docket Number	43614.100

U. S. PATENTS				
Examiner's Initials	Cite No.	Document Number	Issue Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

U. S. PATENT APPLICATION PUBLICATIONS				
Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	Cite No.	Foreign Patent Document <small>(Country Code - Number - Kind)</small>	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	Exhibit D1	ROLF LENDENMANN, "UNDERSTANDING OSF DCE 1.1 FOR AIX AND OS/2, IBM International Technical Support Organization" (Oct. 1995).
	Exhibit D2	TAKAHIRO KIUCHI AND SHIGEKOTO KAIHARA, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," published in the Proceedings of SNDSS 1996.
	Exhibit D3	EDUARDO SOLANA AND JÜRGEN HARMS, "Flexible Internet Secure Transactions Based on Collaborative Domains," Security Protocols Workshop 1997, pp. 37-51.
	Exhibit D4	DAVID M. MARTIN, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).
	Exhibit D5	BRUCE SCHNEIER, "APPLIED CRYPTOGRAPHY" (1996).
	Exhibit D7	BRIAN C. SCHIMPF, "Securing Web Access with DCE," presented at Network and Distributed System Security (Feb. 10-11, 1997).
	Exhibit D8	WARD ROSENBERY, DAVID KENNEY, AND GERRY FISHER, "UNDERSTANDING DCE" (1993).
	Exhibit D9	DANIEL R. MASYS & DIXIE B. BAKER, "Protecting Clinical Data on Web Client Computers: the PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, FL (Nov. 7-11, 1998).

Examiner Signature	/Karin Reichle/	Date Considered	12/14/2011
--------------------	-----------------	-----------------	------------

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 a copy of this form with next communication to applicant.

Search Notes (continued)




Application/Control No. 95/001,792	Applicant(s)/Patent under Reexamination 7,188,180	
Examiner KARIN REICHLE	Art Unit 3992	

SEARCHED			
Class	Subclass	Date	Examiner
None		12/12/12	

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Review of Patented Files Prosecution History	12/12/11	KMR

Reexamination 	Application/Control No. 95/001,792	Applicant(s)/Patent Under Reexamination 7,188,180
	Certificate Date	Certificate Number

Requester Correspondence Address: <input type="checkbox"/> Patent Owner <input checked="" type="checkbox"/> Third Party
HAYNES AND BOONE, LLP IP SECTION 2323 VICTORY AVENUE, SUITE 700 DALLAS, TX 75219

LITIGATION REVIEW <input checked="" type="checkbox"/>	KMR <small>(examiner initials)</small>	12/12/11 <small>(date)</small>
Case Name		Director Initials
VirnetX Inc.v. Cisco Systems, Inc.,et al, Case .No. 6:10-cv-00417 (E.D. Tex.).		MB for IY

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
1.	
2.	
3.	
4.	

Litigation Search Report CRU 3999

Reexam Control No. 95/001,792

TO: Karin Reichle
Location: Central Reexam Unit
Art Unit: 3992
Date: 12/14/11

From: Monica A. Graves
Location: CRU 3999
MDE 5A64
Phone: (571) 272-7253

Case Serial Number: 95/001,792

monica.graves@uspto.gov

Search Notes

Litigation search for U.S. Patent Number **7,188,180** - **Litigation was found.**

- Status (**OPEN**) 6:10cv417 *Virnetx, Inc. v. Cisco Systems, Inc., et al.*
- Status (**CLOSED**) 6:10cv94 *Virnetx, Inc. v. Microsoft Corporation*

- 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.



Date of Printing: Dec 14, 2011

KEYCITE

H US PAT 7188180 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, Assignee: VimetX, Inc. (Mar 06, 2007)

History

Direct History

- H** 1 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135, 2002 WL 31892276 (U.S. PTO Utility Dec 31, 2002) (NO. 09/504783)
Construed by
- H** 2 VimetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)
- H** 3 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK WITHOUT USER ENTERING ANY CRYPTOGRAPHIC INFORMATION, US PAT 6839759, 2005 WL 132324 (U.S. PTO Utility Jan 04, 2005) (NO. 10/702522)
Construed by
- H** 4 VimetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)
- => 5 **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**, US PAT 7188180, 2007 WL 665444 (U.S. PTO Utility Mar 06, 2007) (NO. 10/702486)
Construed by
- H** 6 VimetX, Inc. v. Microsoft Corp., 2009 WL 2370727, 2009 Markman 2370727 (E.D.Tex. Jul 30, 2009) (NO. 6:07CV80) (Markman Order Version)

Court Documents

Verdict and Settlement Summaries (U.S.A.)

E.D.Tex.

- 7 VimetX Inc. v. Microsoft Corp., 2010 WL 1213036 (Verdict and Settlement Summary) (E.D.Tex. Mar. 16, 2010) (NO. 607-CV-80)

Trial Court Documents (U.S.A.)

© 2011 Thomson Reuters. All rights reserved.

E.D.Tex. Trial Pleadings

- 8 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827531 (Trial Pleading) (E.D.Tex. Apr. 5, 2007) **Plaintiff Virnetx Inc.'s First Amended Complaint for Patent infringement** (NO. 607CV80, TJW)
- 9 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827532 (Trial Pleading) (E.D.Tex. May 4, 2007) **Microsoft's Answer, Defenses, and Counterclaims to Virnetx's First Amended Complaint** (NO. 607CV80, LED)
- 10 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827533 (Trial Pleading) (E.D.Tex. May 24, 2007) **Plaintiff Virnetx's Reply to Defendant Microsoft's Counterclaims** (NO. 607CV80, LED)
- 11 VIRNETX INC., Plaintiff, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 2775842 (Trial Pleading) (E.D.Tex. Jun. 10, 2008) **Plaintiff Virnetx Inc.'s and Science Applications International Corporation's First Amended Complaint for Patent Infringement** (NO. 607CV00080)

E.D.Tex. Expert Testimony

- 12 VIRNETX, INC., v. MICROSOFT CORPORATION., 2008 WL 7465386 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **(Report or Affidavit of Mark T. Jones, Ph.D.)** (NO. 07CV00080)
- 13 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465387 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **Exhibit E: Summary of Opinions of Dr. David B. Johnson Regarding Claim Construction** (NO. 607-CV-80, LED)
- 14 VIRNETX, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465388 (Partial Expert Testimony) (E.D.Tex. Dec. 17, 2008) **Oral & Videotaped Deposition of David P. Johnson, Ph.D.** (NO. 607CV80, LED)
- 15 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5631263 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) **(Partial Testimony of Mark T. Jones, Ph.D.)** (NO. 607-CV-80, LED)
- 16 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465389 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) **(Partial Testimony of Mark T. Jones, Ph.D.)** (NO. 607-CV-80, LED)
- 17 VIRNETX INC., Plaintiff, Science Applications International Corporation, Involuntary Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5653416 (Expert Report and Affidavit) (E.D.Tex. Dec. 30, 2008) **Declaration of Mark T. Jones, Ph.D.** (NO. 607CV80, LED)
- 18 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 423638 (Expert Report and Affidavit) (E.D.Tex. Jan. 20, 2009) **Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 19 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732176 (Expert Report and Affidavit)

© 2011 Thomson Reuters. All rights reserved.

- (E.D.Tex. Feb. 3, 2009) **Reply Declaration of Mark T. Jones, Ph.D** (NO. 607CV80, LED)
- 20 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732177 (Expert Report and Affidavit) (E.D.Tex. Feb. 10, 2009) **Reply Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 21 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732178 (Expert Report and Affidavit) (E.D.Tex. Dec. 18, 2009) **Declaration of Dr. Stephen Wicker in Support of Microsoft's Motion for Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607-CV-80, LED)

E.D.Tex. Trial Motions, Memoranda And Affidavits

- 22 VIRNETX INC., Plaintiff , SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5531230 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 30, 2008) **Plaintiff Virnetx Inc.'s Opening Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV00080)
- 23 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155346 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jan. 20, 2009) **Microsoft's Responsive Claim Construction Brief** (NO. 607-CV-80, LED)
- 24 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155347 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 3, 2009) **Plaintiff Virnetx Inc.'s Reply Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV80, LED)
- 25 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155348 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 10, 2009) **Microsoft's Sur-Reply Claim Construction Brief** (NO. 607-CV-80, LED)
- 26 VIRNETX INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 4654324 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Sep. 3, 2009) **Plaintiff Virnetx Inc.'s Response to Defendant Microsoft Corporation's Motion for Clarification to Amend Appendix B to Claim Construction Opinion** (NO. 607CV80(LED))
- 27 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5819696 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 18, 2009) **Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607CV00080)

E.D.Tex. Expert Resumes

- 28 Mark T. Jones, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914105 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of Mark T. Jones** (NO. 07CV00080)
- 29 David B. Johnson, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007

WL 6914106 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of David B. Johnson** (NO. 07CV00080)

E.D.Tex. Trial Filings

- 30 VIRNETX INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2007 WL 4827534 (Trial Filing) (E.D.Tex. Aug. 29, 2007) **Joint Conference Report** (NO. 607CV80, LED)
- 31 VIRNETX INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5356442 (Trial Filing) (E.D.Tex. Oct. 31, 2008) **Joint Claim Construction and Prehearing Statement** (NO. 607CV80, LED)

E.D.Tex. Verdicts, Agreements and Settlements

- 32 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2010 WL 1046839 (Verdict, Agreement and Settlement) (E.D.Tex. Jan. 14, 2010) **Stipulation of Dismissal** (NO. 607-CV-80, LED)
- 33 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2010 WL 1046840 (Verdict, Agreement and Settlement) (E.D.Tex. Jan. 14, 2010) **Joint Stipulation Regarding Microsoft's Inequitable Conduct Counterclaims and Affirmative Defenses** (NO. 607-CV-80, LED)

Dockets (U.S.A.)

E.D.Tex.

- 34 VIRNETX, INC. v. MICROSOFT CORPORATION, NO. 6:07cv00080 (Docket) (E.D.Tex. Feb. 15, 2007)

Expert Court Documents (U.S.A.)

E.D.Tex.

- 35 VirnetX Inc. v. Microsoft Corp., 2010 WL 1213036 (Verdict and Settlement Summary) (E.D.Tex. Mar. 16, 2010) (NO. 607-CV-80)

E.D.Tex. Expert Testimony

- 36 VIRNETX, INC., v. MICROSOFT CORPORATION., 2008 WL 7465386 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **(Report or Affidavit of Mark T. Jones, Ph.D.)** (NO. 07CV00080)
- 37 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465387 (Expert Report and Affidavit) (E.D.Tex. Oct. 31, 2008) **Exhibit E: Summary of Opinions of Dr. David B. Johnson Regarding Claim Construction** (NO. 607-CV-80, LED)
- 38 VIRNETX, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465388 (Partial Expert Testimony) (E.D.Tex. Dec. 17, 2008) **Oral & Videotaped Deposition of David**

© 2011 Thomson Reuters. All rights reserved.

- P. Johnson, Ph.D.** (NO. 607CV80, LED)
- 39 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5631263 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 40 VIRNETX, INC. and Science Application International Corporation, Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2008 WL 7465389 (Partial Expert Testimony) (E.D.Tex. Dec. 19, 2008) (**Partial Testimony of Mark T. Jones, Ph.D.**) (NO. 607-CV-80, LED)
- 41 VIRNETX INC., Plaintiff, Science Applications International Corporation, Involuntary Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5653416 (Expert Report and Affidavit) (E.D.Tex. Dec. 30, 2008) **Declaration of Mark T. Jones, Ph.D.** (NO. 607CV80, LED)
- 42 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 423638 (Expert Report and Affidavit) (E.D.Tex. Jan. 20, 2009) **Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 43 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732176 (Expert Report and Affidavit) (E.D.Tex. Feb. 3, 2009) **Reply Declaration of Mark T. Jones, Ph.D** (NO. 607CV80, LED)
- 44 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732177 (Expert Report and Affidavit) (E.D.Tex. Feb. 10, 2009) **Reply Declaration of David B. Johnson, Ph.D., Regarding Claim Construction** (NO. 607-CV-80, LED)
- 45 VIRNETX, INC. and Science, Applications International Corp., Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 5732178 (Expert Report and Affidavit) (E.D.Tex. Dec. 18, 2009) **Declaration of Dr. Stephen Wicker in Support of Microsoft's Motion for Summary Judgment of Invalidity of U.S. Patent No. 6,839,759** (NO. 607-CV-80, LED)

E.D.Tex. Trial Motions, Memoranda And Affidavits

- 46 VIRNETX INC., Plaintiff, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, Involuntary plaintiff, v. MICROSOFT CORPORATION, Defendant., 2008 WL 5531230 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Dec. 30, 2008) **Plaintiff Virnetx Inc.'s Opening Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV00080)
- 47 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155346 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Jan. 20, 2009) **Microsoft's Responsive Claim Construction Brief** (NO. 607-CV-80, LED)
- 48 VIRNETX INC., Plaintiff, Science Applications International Corporation Involuntary, Plaintiff, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155347 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 3, 2009) **Plaintiff Virnetx Inc.'s Reply Brief in Support of Its Construction of Claims Pursuant to P.R. 4-5** (NO. 607CV80, LED)
- 49 VIRNETX, INC. and Science Applications International Corp., Plaintiffs, v. MICROSOFT CORPORATION, Defendant., 2009 WL 1155348 (Trial Motion, Memorandum and Affidavit) (E.D.Tex. Feb. 10, 2009) **Microsoft's Sur-Reply Claim Construction Brief** (NO. 607-CV-80,

LED)

E.D.Tex. Expert Resumes

- 50 Mark T. Jones, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914105 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of Mark T. Jones** (NO. 07CV00080)
- 51 David B. Johnson, Ph.D., curriculum vitae filed in VirnetX, Inc. v. Microsoft Corporation, 2007 WL 6914106 (Court-filed Expert Resume) (E.D.Tex. 2007) **Expert Resume of David B. Johnson** (NO. 07CV00080)

Patent Family

- 52 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

- 53 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Number of Pages: 005, (DATE RECORDED: Jan 10, 2007)
- 54 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Number of Pages: 003, (DATE RECORDED: Nov 07, 2003)

Patent Status Files

- .. Request for Re-Examination, (OG DATE: Dec 13, 2011)
- .. Re-Examination Certificate, (OG DATE: Jun 07, 2011)
- .. Request for Re-Examination, (OG DATE: Mar 02, 2010)
- .. Certificate of Correction, (OG DATE: Aug 28, 2007)

Docket Summaries

- 59 VIRNETX INC. v. CISCO SYSTEMS, INC. ET AL, (E.D.TEX. Aug 11, 2010) (NO. 6:10CV00417), (35 USC 271 PATENT INFRINGEMENT)
- 60 VIRNETX INC. v. MICROSOFT CORPORATION, (E.D.TEX. Mar 17, 2010) (NO. 6:10CV00094), (35 USC 271 PATENT INFRINGEMENT)

Litigation Alert

- 61 Derwent LitAlert P2010-35-19 (Aug 11, 2010) Action Taken: complaint for PATENT INFRINGEMENT
- 62 Derwent LitAlert P2010-13-31 (Mar 17, 2010) Action Taken: complaint

Prior Art (Coverage Begins 1976)

- C** 63 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 7010604 Assignee: Science Applications International, (U.S. PTO Utility 2006)
- H** 64 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135 Assignee: Science Applications International, (U.S. PTO Utility 2002)
- C** 65 APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM, US PAT 5787172 Assignee: The Merdan Group, Inc., (U.S. PTO Utility 1998)
- C** 66 AUTOCONFIGURABLE METHOD AND SYSTEM HAVING AUTOMATED DOWNLOADING, US PAT 5870610 Assignee: Siemens Business Communication Systems,, (U.S. PTO Utility 1999)
- C** 67 CRYPTOGRAPHIC KEY MANAGEMENT APPARATUS AND METHOD, US PAT 5341426 Assignee: Motorola, Inc., (U.S. PTO Utility 1994)
- C** 68 DOMAIN NAME ROUTING, US PAT 6119171 Assignee: IP Dynamics, Inc., (U.S. PTO Utility 2000)
- C** 69 DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION, US PAT 6332158 (U.S. PTO Utility 2001)
- C** 70 DYNAMIC NETWORK ADDRESS UPDATING, US PAT 6243749 Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2001)
- C** 71 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6052788 Assignee: Network Engineering Software, Inc., (U.S. PTO Utility 2000)
- C** 72 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 5898830 Assignee: Network Engineering Software, (U.S. PTO Utility 1999)
- C** 73 MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS, US PAT 5905859 Assignee: International Business Machines, (U.S. PTO Utility 1999)
- C** 74 METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION, US PAT 5796942 Assignee: Computer Associates International, Inc., (U.S. PTO Utility 1998)
- C** 75 METHOD AND APPARATUS FOR CLIENT-HOST COMMUNICATION OVER A COMPUTER NETWORK, US PAT 6119234 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 2000)
- C** 76 METHOD AND APPARATUS FOR CONFIGURING A VIRTUAL PRIVATE NETWORK, US PAT 6226751 Assignee: VPN Technologies, Inc., (U.S. PTO Utility 2001)
- C** 77 METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM, US PAT 5892903 Assignee: Internet Security Systems, Inc., (U.S. PTO Utility 1999)
- C** 78 METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM, US PAT 6006259 Assignee: Network Alchemy, Inc., (U.S. PTO Utility 1999)

© 2011 Thomson Reuters. All rights reserved.

- C** 79 METHOD AND APPARATUS FOR A KEY-MANAGEMENT SCHEME FOR INTERNET PROTOCOLS, US PAT 5588060 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1996)
- C** 80 METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK, US PAT 6079020 Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2000)
- C** 81 METHOD AND APPARATUS FOR PROVIDING NETWORK ACCESS CONTROL USING A DOMAIN NAME SYSTEM, US PAT 6256671 Assignee: Nortel Networks Limited, (U.S. PTO Utility 2001)
- C** 82 METHOD AND APPARATUS FOR PROVIDING A VIRTUAL PRIVATE NETWORK, US PAT 6092200 Assignee: Novell, Inc., (U.S. PTO Utility 2000)
- C** 83 METHOD AND PROTOCOL FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION, US PAT 6353614 Assignee: 3Com Corporation, (U.S. PTO Utility 2002)
- C** 84 METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES, US PAT 6286047 Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)
- H** 85 MULTI-ACCESS VIRTUAL PRIVATE NETWORK, US PAT 6158011 Assignee: V-One Corporation, (U.S. PTO Utility 2000)
- C** 86 NETWORK COMMUNICATIONS ADAPTER WITH DUAL INTERLEAVED MEMORY BANKS SERVICING MULTIPLE PROCESSORS, US PAT 4933846 Assignee: Network Systems Corporation, (U.S. PTO Utility 1990)
- C** 87 NETWORK WITH SECURE COMMUNICATIONS SESSIONS, US PAT 5689566 (U.S. PTO Utility 1997)
- H** 88 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 5842040 Assignee: Storage Technology Corporation, (U.S. PTO Utility 1998)
- C** 89 SECURE DELIVERY OF INFORMATION IN A NETWORK, US PAT 6178505 Assignee: Internet Dynamics, Inc., (U.S. PTO Utility 2001)
- C** 90 SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY, US PAT 5805801 Assignee: International Business Machines, (U.S. PTO Utility 1998)
- C** 91 SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS, US PAT 6330562 Assignee: International Business Machines, (U.S. PTO Utility 2001)
- C** 92 SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE, US PAT 5878231 Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1999)
- C** 93 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR MULTIPLE-ENTRY POINT VIRTUAL POINT OF SALE ARCHITECTURE, US PAT 6178409 Assignee: VeriFone, Inc., (U.S. PTO Utility 2001)
- C** 94 VIRTUAL PRIVATE NETWORK SYSTEM OVER PUBLIC MOBILE DATA NETWORK AND VIRTUAL LAN, US PAT 6016318 Assignee: NEC Corporation, (U.S. PTO Utility 2000)

© 2011 Thomson Reuters. All rights reserved.

US District Court Civil Docket

**U.S. District - Texas Eastern
(Tyler)**

6:10cv417

Virnetx Inc v. Cisco Systems, Inc et al

This case was retrieved from the court on Wednesday, December 14, 2011

Date Filed: 08/11/2010 **Class Code:**
Assigned To: Judge Leonard Davis **Closed: No**
Referred To: **Statute: 35:271**
Nature of suit: Patent (830) **Jury Demand: Both**
Cause: Patent Infringement **Demand Amount: \$0**
Lead Docket: None **NOS Description: Patent**
Other Docket: None
Jurisdiction: Federal Question

Litigants

Attorneys

Honorable Robert Faulkner
Mediator

Robert W Faulkner
[COR LD NTC]
Jams Inc
8401 N Central Expressway
Suite 610
Dallas, TX 75225
USA
214/ 744-5267
Fax: 214/ 720-6010
Email: RFAULKNER@JAMSADR.COM

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler, TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

John Austin Curry
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4207
Fax: 214-978-4044
Email: ACURRY@MCKOOLSMITH.COM

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Mitchell Reed Sibley

[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: MSIBLEY@MCKOOLSMITH.COM

Ramzi Ragheb Khazen
[COR LD NTC]
McKool Smith -Austin
300 W 6TH St
Ste 1700
Austin , TX 78701
USA
512-692-8743
Fax: 512-692-8744
Email: RKHAZEN@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKOOLSMITH.COM

Cisco Systems, Inc
Defendant

Allen Franklin Gardner
[COR LD NTC]
Potter Minton PC

110 N College
Suite 500
PO Box 359
Tyler , TX 75710-0359
USA
903/ 597-8311
Email: Allengardner@potterminton.com

Ameet A Modi
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: AMODI@DESMARAISLLP.COM

Andrew G Hamill
[COR LD NTC]
Bridges & Mavrakakis
540 Cowper Street
Suite 100
Palo Alto , CA 94301
USA
415/ 439-1958
Fax: 415/ 439-1550
Email: AHAMILL@BRIDGESMAV.COM

Bradford J Black
[COR LD NTC]
Black Chang & Hamill LLP
333 Bush Street
Suite 2250
San Francisco , CA 94104
USA
415/ 369-9423
Fax: 415/ 520-6840
Email: BBLACK@BCHLLP.COM

Dmitriy Kheyfits
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: DKHEYFITS@DESMARAISLLP.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

John M Desmarais
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue

New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: JDESMARAIS@DESMARAISLLP.COM

Karim Z Oussayef
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3427
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: KOUSSAYEF@DESMARAISLLP.COM

Michael E Jones
[COR LD NTC]
Potter Minton PC
110 N College
Suite 500
PO Box 359
Tyler , TX 75710-0359
USA
903-597-8311
Fax: 903-593-0846
Email: MIKEJONES@POTTERMINTON.COM

Michael P Stadnick
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: MSTADNICK@DESMARAISLLP.COM

Peter H Chang
[COR LD NTC]
Black Chang & Hamill LLP
333 Bush Street
Suite 2250
San Francisco , CA 94104
USA
415-369-9423
Fax: 415-520-6840
Email: PCHANG@BCHLLP.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Tamir Packin
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue

Apple Inc
Defendant

New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: TPACKIN@DESMARAISLLP.COM

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

Eric Miller Albritton
[COR LD NTC]
Albritton Law Firm
PO Box 2649
111 West Tyler, 75601
Longview , TX 75606
USA
(903) 757-8449
Fax: (903) 758-7397
Email: EMA@EMAFIRM.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Kyung Kim
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4080
Fax: 713/ 934-7011
Email: DKIM@WMALAW.COM

Matthew Richard Rodgers
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4061
Email: Mrodgers@wmalaw.com

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101

Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Ruben Singh Bains
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4064
Fax: 713/ 934-7011
Email: Rbains@wmalaw.com

Aastra Technologies Ltd
Defendant

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Nec Corporation
Defendant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1700
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700

Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1838
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Nec Corporation of America
Defendant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1700
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1838
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Aastra USA, Inc
Defendant

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Science Applications International Corporation
Movant

Andy Tindel
[COR LD NTC]
Provost Umphrey Law Firm -Tyler
112 E Line
Suite 304
Tyler , TX 75702
USA
903/ 596-0900
Fax: 903/ 596-0909
Email: Atindel@andytindel.com

Nec Corporation of America
Counter Claimant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1700
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1838
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Nec Corporation
Counter Claimant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1700
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington

875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1838
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court

Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702

USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Cisco Systems, Inc
Counter Claimant

Ameet A Modi
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: AMODI@DESMARAISSLP.COM

Andrew G Hamill
[COR LD NTC]
Bridges & Mavrakakis
540 Cowper Street
Suite 100
Palo Alto , CA 94301
USA
415/ 439-1958
Fax: 415/ 439-1550
Email: AHAMILL@BRIDGESMAV.COM

Bradford J Black
[COR LD NTC]
Black Chang & Hamill LLP
333 Bush Street
Suite 2250
San Francisco , CA 94104
USA
415/ 369-9423
Fax: 415/ 520-6840
Email: BBLACK@BCHLLP.COM

Dmitriy Kheyfits
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: DKHEYFITS@DESMARAISSLP.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA

903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

John M Desmarais
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: JDESMARAIS@DESMARAISLLP.COM

Karim Z Oussayef
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3427
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: KOUSSAYEF@DESMARAISLLP.COM

Michael P Stadnick
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: MSTADNICK@DESMARAISLLP.COM

Peter H Chang
[COR LD NTC]
Black Chang & Hamill LLP
333 Bush Street
Suite 2250
San Francisco , CA 94104
USA
415-369-9423
Fax: 415-520-6840
Email: PCHANG@BCHLLP.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Tamir Packin
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401

Virnetx Inc
Counter Defendant

<i>pro Hac Vice</ I>
Email: TPACKIN@DESMARAISSL.P.COM

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000 .

Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Apple Inc
Counter Claimant

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

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Kyung Kim
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4080
Fax: 713/ 934-7011
Email: DKIM@WMALAW.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Ruben Singh Bains
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4064
Fax: 713/ 934-7011
Email: Rbains@wmalaw.com

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter

Aastra Technologies Ltd
Counter Claimant

[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith

300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114

Aastra USA, Inc
Counter Claimant

Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA

903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687

Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Aastra USA, Inc
Counter Claimant

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000 -
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt

[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler, TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler, TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall, TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas, TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKOOLSMITH.COM

Aastra Technologies Ltd
Counter Claimant

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas, TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana, TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300

Virnetx Inc
Counter Defendant

Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500

Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKOOLSMITH.COM

Nec Corporation of America
Counter Claimant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700

Fax: 202/ 551-1700
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1838
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Nec Corporation
Counter Claimant

Bhaskar Kakarla
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-1700
Email: BHASKARKAKARLA@PAULHASTINGS.COM

Brock S Weber
[COR LD NTC]
Paul Hastings Janofsky & Walker -Washington
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1700
Fax: 202/ 551-0183
<i>pro Hac Vice</ I>
Email: BROCKWEBER@PAULHASTINGS.COM

Douglas Ray McSwane , Jr
[COR LD NTC]
Potter Minton
P O Box 359
Tyler , TX 75710
USA
903/ 597/ 8311
Fax: 9035930846
Email: DOUGMCSWANE@POTTERMINTON.COM

Robert M Masters
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1763
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: ROBMASTERS@PAULHASTINGS.COM

Timothy P Cremen
[COR LD NTC]
Paul Hastings LLP
875 15TH Street NW
Washington , DC 20005
USA
202/ 551-1838
Fax: 202/ 551-1700
<i>pro Hac Vice</ I>
Email: TIMOTHYCREMEN@PAULHASTINGS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]

McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKOOLSMITH.COM

Apple Inc
Counter Claimant

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

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Kyung Kim
[COR LD NTC]
Williams Morgan & Amerson PC
10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4080
Fax: 713/ 934-7011
Email: DKIM@WMALAW.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Ruben Singh Bains
[COR LD NTC]
Williams Morgan & Amerson PC

Virnetx Inc
Counter Defendant

10333 Richmond
Suite 1100
Houston , TX 77042
USA
713/ 934-4064
Fax: 713/ 934-7011
Email: Rbains@wmalaw.com

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas

300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKOOLSMITH.COM

Cisco Systems, Inc
Counter Claimant

Allen Franklin Gardner
[COR LD NTC]
Potter Minton PC
110 N College
Suite 500

PO Box 359
Tyler, TX 75710-0359
USA
903/ 597-8311
Email: Allengardner@potterminton.com

Ameet A Modi
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York, NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: AMODI@DESMARAISLLP.COM

Andrew G Hamill
[COR LD NTC]
Bridges & Mavrakakis
540 Cowper Street
Suite 100
Palo Alto, CA 94301
USA
415/ 439-1958
Fax: 415/ 439-1550
Email: AHAMILL@BRIDGESMAV.COM

Bradford J Black
[COR LD NTC]
Black Chang & Hamill LLP
333 Bush Street
Suite 2250
San Francisco, CA 94104
USA
415/ 369-9423
Fax: 415/ 520-6840
Email: BBLACK@BCHLLP.COM

Dmitriy Kheyfits
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York, NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: DKHEYFITS@DESMARAISLLP.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler, TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

John M Desmarais
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York, NY 10169
USA

212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: JDESMARAIS@DESMARAISLLP.COM

Karim Z Oussayef
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3427
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: KOUSSAYEF@DESMARAISLLP.COM

Michael E Jones
[COR LD NTC]
Potter Minton PC
110 N College
Suite 500
PO Box 359
Tyler , TX 75710-0359
USA
903-597-8311
Fax: 903-593-0846
Email: MIKEJONES@POTTERMINTON.COM

Michael P Stadnick
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA
212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: MSTADNICK@DESMARAISLLP.COM

Peter H Chang
[COR LD NTC]
Black Chang & Hamill LLP
333 Bush Street
Suite 2250
San Francisco , CA 94104
USA
415-369-9423
Fax: 415-520-6840
Email: PCHANG@BCHLLP.COM

Roger Brian Craft
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: BCRAFT@FINDLAYCRAFT.COM

Tamir Packin
[COR LD NTC]
Desmarais LLP -New York
230 Park Avenue
New York , NY 10169
USA

Virnetx Inc
Counter Defendant

212/ 351-3400
Fax: 212/ 351-3401
<i>pro Hac Vice</ I>
Email: TPACKIN@DESMARAISLLP.COM

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201

USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKOOLSMITH.COM

Aastra USA, Inc
Counter Claimant

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826

Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 9035339687
Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
[COR LD NTC]
McKool Smith -Marshall P O Box O
104 East Houston St, Suite 300
Marshall , TX 75670
USA
903/ 923-9000
Fax: 903-923-9099
Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
[COR LD NTC]

Aastra Technologies Ltd
Counter Claimant

McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4259
Fax: 214/ 978-4044
Email: SGRESKOWIAK@MCKKOOLSMITH.COM

Jon Bentley Hyland
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
214-580-3826
Email: JHYLAND@PATTONROBERTS.COM

Phillip Nollin Cockrell
[COR LD NTC]
Patton Roberts PLLC -Texarkana
2900 St Michael Drive, Suite 400
Texarkana , TX 75503
USA
903/ 334-7107
Fax: 903-334-7007
Email: PCOCKRELL@PATTONROBERTS.COM

Robert David Katz
[COR LD NTC]
Patton Roberts, PLLC
901 Main Street
Ste 3300
Dallas , TX 75201
USA
972-998-5856
Fax: 214-377-3622
Email: RKATZ@PATTONROBERTS.COM

Virnetx Inc
Counter Defendant

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

Andrew Thompson Gorham
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903.531.3535
Fax: 903.533.9687
Email: TGORHAM@PBATYLER.COM

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith

300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Charles Ainsworth
[COR LD NTC]
Parker Bunt & Ainsworth
100 E Ferguson
Suite 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Charley@pbatyler.com

Daniel R Pearson
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4217
Fax: 214-978-4044
Email: DPEARSON@MCKOOLSMITH.COM

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Robert Christopher Bunt
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 East Ferguson, Ste 1114
Tyler , TX 75702
USA
903/ 531-3535
Fax: 903/ 533-9687
Email: Rcbunt@pbatyler.com

Robert M Parker
[COR LD NTC]
Parker, Bunt & Ainsworth, PC
100 E Ferguson
Suite 1114

Tyler , TX 75702
 USA
 903/ 531-3535
 Fax: 9035339687
 Email: Rmparker@pbatyler.com

Samuel Franklin Baxter
 [COR LD NTC]
 McKool Smith -Marshall P O Box O
 104 East Houston St, Suite 300
 Marshall , TX 75670
 USA
 903/ 923-9000
 Fax: 903-923-9099
 Email: Sbaxter@mckoolsmith.com

Stacie Lynn Greskowiak
 [COR LD NTC]
 McKool Smith -Dallas
 300 Crescent Court
 Suite 1500
 Dallas , TX 75201
 USA
 214/ 978-4259
 Fax: 214/ 978-4044
 Email: SGRESKOWIAK@MCKOOLSMITH.COM

Date	#	Proceeding Text	Source
08/11/2010	1	COMPLAINT against Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America (Filing fee \$ 350 receipt number 0540-2618483.), filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Exhibit E, # 6 Civil Cover Sheet)(Cawley, Douglas) (Entered: 08/11/2010)	
08/11/2010	--	Judge Leonard Davis added. (mll,) (Entered: 08/12/2010)	
08/12/2010	2	CORPORATE DISCLOSURE STATEMENT filed by VirnetX Inc. identifying Corporate Parent VirnetX Holding Corporation for VirnetX Inc.. (Cawley, Douglas) (Entered: 08/12/2010)	
08/12/2010	3	E-GOV SEALED SUMMONS Issued as to Apple Inc. (kls,) (Entered: 08/12/2010)	
08/12/2010	4	E-GOV SEALED SUMMONS Issued as to Aastra Technologies Ltd. (kls,) (Entered: 08/12/2010)	
08/12/2010	5	E-GOV SEALED SUMMONS Issued as to Cisco Systems, Inc. (kls,) (Entered: 08/12/2010)	
08/12/2010	6	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: 08/12/2010)	
08/12/2010	7	E-GOV SEALED SUMMONS Issued as to NEC Corporation. (kls,) (Entered: 08/12/2010)	
08/12/2010	8	E-GOV SEALED SUMMONS Issued as to Aastra USA, Inc. (kls,) (Entered: 08/12/2010)	
08/12/2010	9	E-GOV SEALED SUMMONS Issued as to NEC Corporation of America. (kls,) (Entered: 08/12/2010)	
08/17/2010	10	NOTICE of Attorney Appearance by Samuel Franklin Baxter on behalf of VirnetX Inc. (Baxter, Samuel) (Entered: 08/17/2010)	
08/17/2010	11	NOTICE of Attorney Appearance by Luke Fleming McLeroy on behalf of VirnetX Inc. (McLeroy, Luke) (Entered: 08/17/2010)	
08/17/2010	12	NOTICE of Attorney Appearance by Bradley Wayne Caldwell on behalf of VirnetX Inc. (Caldwell, Bradley) (Entered: 08/17/2010)	

- 08/17/2010 13 NOTICE of Attorney Appearance by Jason Dodd Cassady on behalf of VirnetX Inc. (Cassady, Jason) (Entered: 08/17/2010)
- 09/01/2010 14 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint, or Otherwise Respond by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Craft, Roger) (Entered: 09/01/2010)
- 09/01/2010 15 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint, by Apple Inc.. (Attachments: # 1 Text of Proposed Order)(Craft, Roger) (Entered: 09/01/2010)
- 09/01/2010 16 NOTICE of Attorney Appearance by Eric Hugh Findlay on behalf of Cisco Systems, Inc. (Findlay, Eric) (Entered: 09/01/2010)
- 09/01/2010 17 NOTICE of Attorney Appearance by Eric Hugh Findlay on behalf of Apple Inc. (Findlay, Eric) (Entered: 09/01/2010)
- 09/02/2010 18 ORDER granting 14 Motion for Extension of Time to Answer. Deft Cisco Systems Inc shall have to 10-29-2010 to move, answer, or otherwise respond to pltf's Complaint. Signed by Judge Leonard Davis on 09/02/10. cc:attys 9-02-10 (mll,) (Entered: 09/02/2010)
- 09/02/2010 19 ORDER granting 15 Motion for Extension of Time to Answer. Deft Apple Inc shall have to 10-29-2010 to move, answer, or otherwise respond to pltf's Complaint. Signed by Judge Leonard Davis on 09/02/10. cc:attys 9-02-10 (mll,) (Entered: 09/02/2010)
- 09/03/2010 20 NOTICE of Attorney Appearance by Phillip Nollin Cockrell on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Cockrell, Phillip) (Entered: 09/03/2010)
- 09/03/2010 21 NOTICE of Attorney Appearance by Robert David Katz on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Katz, Robert) (Entered: 09/03/2010)
- 09/03/2010 22 NOTICE of Attorney Appearance by Jon Bentley Hyland on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Hyland, Jon) (Entered: 09/03/2010)
- 09/03/2010 23 DOCUMENT FILED IN ERROR. PLEASE DISREGARD.*** Defendant's Unopposed First Application for Extension of Time to Answer, Move or Otherwise Respond to Complaint re Aastra Technologies Ltd., Aastra USA, Inc..(Hyland, Jon) Modified on 9/7/2010 (mjc,). (Entered: 09/03/2010)
- 09/03/2010 27 APPLICATION to Appear Pro Hac Vice by Attorney Robert M Masters for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/07/2010)
- 09/03/2010 28 APPLICATION to Appear Pro Hac Vice by Attorney Bhaskar Kakarla for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/07/2010)
- 09/03/2010 29 APPLICATION to Appear Pro Hac Vice by Attorney Brock S Weber for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/07/2010)
- 09/07/2010 -- ***FILED IN ERROR. Document # 23 , Defendant's First Unopposed Application for Extension of Time. DOCUMENT FILED USING INCORRECT DOCKET EVENT. PLEASE IGNORE.*** (mjc,) (Entered: 09/07/2010)
- 09/07/2010 24 Agreed MOTION for Extension of Time to File Answer re 1 Complaint, by Aastra Technologies Ltd., Aastra USA, Inc.. (Attachments: # 1 Text of Proposed Order)(Hyland, Jon) (Entered: 09/07/2010)
- 09/07/2010 25 E-GOV SEALED SUMMONS Issued as to NEC Corporation of America. (kls,) (Entered: 09/07/2010)
- 09/07/2010 26 E-GOV SEALED SUMMONS Issued as to NEC Corporation. (kls,) (Entered: 09/07/2010)
- 09/08/2010 30 ORDER granting 24 Motion for Extension of Time to Answer. Aastra defts will have to 10-29-2010 to answer, move or otherwise respond to pltf's Complaint. Signed by Judge Leonard Davis on 09/08/10. cc:attys 9-08-10 (mll,) (Entered: 09/08/2010)
- 09/09/2010 31 NOTICE of Attorney Appearance by Robert M Parker on behalf of VirnetX Inc. (Parker, Robert) (Entered: 09/09/2010)
- 09/09/2010 32 NOTICE of Attorney Appearance by Robert Christopher Bunt on behalf of VirnetX Inc. (Bunt, Robert) (Entered: 09/09/2010)
- 09/09/2010 33 NOTICE of Attorney Appearance by Charles Ainsworth on behalf of VirnetX Inc. (Ainsworth, Charles) (Entered: 09/09/2010)

- 09/09/2010 34 NOTICE of Attorney Appearance by Andrew Thompson Gorham on behalf of VirnetX Inc. (Gorham, Andrew) (Entered: 09/09/2010)
- 09/09/2010 35 NOTICE of Attorney Appearance by Daniel R Pearson on behalf of VirnetX Inc. (Pearson, Daniel) (Entered: 09/09/2010)
- 09/16/2010 36 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Aastra Technologies Ltd. personally served on 8/20/2010 by Process Server Andrew Kovacs on Jamshid Rezaei, Director IT designated to accept process of service, answer due 9/10/2010. (ehs,) (Entered: 09/16/2010)
- 09/16/2010 37 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Aastra USA, Inc. personally served on Sue Vertrees designated by law to accept process of service served on 8/18/2010, answer due 9/8/2010. (ehs,) (Entered: 09/16/2010)
- 09/16/2010 38 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Apple Inc. served on 8/18/2010 by serving Registered Agent Meagan Nichols, answer due 9/8/2010. (ehs,) (Entered: 09/16/2010)
- 09/16/2010 39 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. Cisco Systems, Inc. personally served on 8/18/2010 Bradley Ellison, person authorized to accept service of process, answer due 9/8/2010. (ehs,) (Entered: 09/16/2010)
- 09/16/2010 40 E-GOV SEALED SUMMONS Returned Executed by VirnetX Inc.. NEC Corporation of America personally served on 8/19/2010 on Dionne Miles, Managing Agent authorized by law to accept service of process, answer due 9/9/2010. (ehs,) (Entered: 09/16/2010)
- 09/16/2010 41 APPLICATION to Appear Pro Hac Vice by Attorney Timothy P Cremen for NEC Corporation, NEC Corporation of America. (mll,) (Entered: 09/16/2010)
- 09/28/2010 42 NEC Corporation's Unopposed First Application for Extension of Time to Answer Complaint (McSwane, Douglas). (Entered: 09/28/2010)
- 09/28/2010 43 NEC Corporation of America's Unopposed First Application for Extension of Time to Answer Complaint (McSwane, Douglas) (Entered: 09/28/2010)
- 09/29/2010 -- Defendant's Unopposed First Application for Extension of Time to Answer Complaint 42 is granted pursuant to Local Rule CV-12 for NEC Corporation to 10/29/2010. 10 Days Granted for Deadline Extension.(mll,) (Entered: 09/29/2010)
- 09/29/2010 -- Defendant's Unopposed First Application for Extension of Time to Answer Complaint 43 is granted pursuant to Local Rule CV-12 for NEC Corporation of America to 10/29/2010. 30 Days Granted for Deadline Extension.(mll,) (Entered: 09/29/2010)
- 10/06/2010 44 NOTICE of Attorney Appearance by Danny Lloyd Williams on behalf of Apple Inc. (Williams, Danny) (Entered: 10/06/2010)
- 10/06/2010 45 NOTICE of Attorney Appearance by Ruben Singh Bains on behalf of Apple Inc. (Bains, Ruben) (Entered: 10/06/2010)
- 10/06/2010 46 NOTICE of Attorney Appearance by Kyung Kim on behalf of Apple Inc. (Kim, Kyung) (Entered: 10/06/2010)
- 10/26/2010 47 APPLICATION to Appear Pro Hac Vice by Attorney Tamir Packin for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)
- 10/26/2010 48 APPLICATION to Appear Pro Hac Vice by Attorney Ameet A Modi for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)
- 10/26/2010 49 APPLICATION to Appear Pro Hac Vice by Attorney Dmitriy Kheyfits for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)
- 10/26/2010 50 APPLICATION to Appear Pro Hac Vice by Attorney John M Desmarais for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)
- 10/26/2010 51 APPLICATION to Appear Pro Hac Vice by Attorney Michael P Stadnick for Cisco Systems, Inc.. (mll,) (Entered: 10/26/2010)
- 10/29/2010 52 NEC Corp and NEC Corp of America's ANSWER to 1 Complaint, and , COUNTERCLAIM against VirnetX Inc. by NEC Corporation of America, NEC Corporation.(McSwane, Douglas) (Entered: 10/29/2010)

- 10/29/2010 53 Cisco Systems, Inc.'s ANSWER to 1 Complaint, and , COUNTERCLAIM against VirnetX Inc. by Cisco Systems, Inc..(Findlay, Eric) (Entered: 10/29/2010)
- 10/29/2010 54 CORPORATE DISCLOSURE STATEMENT filed by Cisco Systems, Inc. identifying Corporate Parent None for Cisco Systems, Inc.. (Findlay, Eric) (Entered: 10/29/2010)
- 10/29/2010 55 ANSWER to 1 Complaint, AFFIRMATIVE DEFENSES , COUNTERCLAIM against VirnetX Inc. by Apple Inc..(Williams, Danny) (Entered: 10/29/2010)
- 10/29/2010 56 CORPORATE DISCLOSURE STATEMENT filed by Apple Inc. (Williams, Danny) (Entered: 10/29/2010)
- 10/29/2010 57 Aastra Technologies Limited's ANSWER to 1 Complaint, AFFIRMATIVE DEFENSES , COUNTERCLAIM against VirnetX Inc. by Aastra Technologies Ltd.. (Cockrell, Phillip) (Entered: 10/29/2010)
- 10/29/2010 58 CORPORATE DISCLOSURE STATEMENT filed by Aastra Technologies Ltd. (Cockrell, Phillip) (Entered: 10/29/2010)
- 10/29/2010 59 Aastra USA Inc's ANSWER to 1 Complaint, AFFIRMATIVE DEFENSES , COUNTERCLAIM against VirnetX Inc. by Aastra USA, Inc..(Cockrell, Phillip) (Entered: 10/29/2010)
- 10/29/2010 60 CORPORATE DISCLOSURE STATEMENT filed by Aastra USA, Inc. (Cockrell, Phillip) (Entered: 10/29/2010)
- 11/02/2010 61 CORPORATE DISCLOSURE STATEMENT filed by NEC Corporation, NEC Corporation of America (McSwane, Douglas) (Entered: 11/02/2010)
- 11/05/2010 62 APPLICATION to Appear Pro Hac Vice by Attorney Andrew G Hamill for Cisco Systems, Inc. (mll,) (Entered: 11/05/2010)
- 11/05/2010 63 APPLICATION to Appear Pro Hac Vice by Attorney Bradford J Black for Cisco Systems, Inc. (mll,) (Additional attachment(s) added on 11/8/2010: # 1 Exhibit) (mll,). (Entered: 11/05/2010)
- 11/22/2010 64 ANSWER to 53 Answer to Complaint, Counterclaim by VirnetX Inc..(Cawley, Douglas) (Entered: 11/22/2010)
- 11/22/2010 65 ANSWER to 52 Answer to Complaint, Counterclaim by VirnetX Inc..(Cawley, Douglas) (Entered: 11/22/2010)
- 11/22/2010 66 ANSWER to 55 Answer to Complaint, Counterclaim by VirnetX Inc..(Cawley, Douglas) (Entered: 11/22/2010)
- 11/22/2010 67 ANSWER to 57 Answer to Complaint, Counterclaim by VirnetX Inc..(Cawley, Douglas) (Entered: 11/22/2010)
- 11/22/2010 68 ANSWER to 59 Answer to Complaint, Counterclaim by VirnetX Inc..(Cawley, Douglas) (Entered: 11/22/2010)
- 01/04/2011 69 NOTICE by VirnetX Inc. NOTICE REGARDING A SCHEDULING CONFERENCE (Cawley, Douglas) (Entered: 01/04/2011)
- 01/12/2011 70 ORDER setting Status Conference for 2/7/2011 01:30 PM before Judge Leonard Davis and Judge John Love. Signed by Judge Leonard Davis on 01/12/11. cc:attys 1-12-11(mll,) (Entered: 01/12/2011)
- 01/14/2011 71 NOTICE of Designation of Attorney in Charge to Jon Bentley Hyland on behalf of Aastra Technologies Ltd., Aastra USA, Inc. (Hyland, Jon) (Entered: 01/14/2011)
- 01/17/2011 72 NOTICE of Attorney Appearance by Stacie Lynn Greskowiak on behalf of VirnetX Inc. (Greskowiak, Stacie) (Entered: 01/17/2011)
- 01/24/2011 73 NOTICE of Attorney Appearance by Michael E Jones on behalf of Cisco Systems, Inc. (Jones, Michael) (Entered: 01/24/2011)
- 01/24/2011 74 NOTICE of Attorney Appearance by Allen Franklin Gardner on behalf of Cisco Systems, Inc. (Gardner, Allen) (Entered: 01/24/2011)
- 02/04/2011 75 AMENDED COMPLAINT against Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America, filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Exhibit E)(Cawley, Douglas) (Entered: 02/04/2011)
- 02/07/2011 76 2.7.11 Minute Entry - Status Conference: for proceedings held before Judge

- Leonard Davis and Judge John Love: Status Conference held on 2/7/2011.
(Court Reporter Shea Sloan.) (Attachments: # 1 Attorney Sign-In Sheets)
(rlf,) (Entered: 02/11/2011)
- 02/07/2011 -- ELECTRONIC Minute Entry for proceedings held before Magistrate Judge John D. Love and Judge Davis: Status Conference held on 2/7/2011. (refer to document #76) (Court Reporter Shea Sloan.) (mjm,) (Entered: 02/14/2011)
- 02/14/2011 77 NOTICE by VirnetX Inc. VIRNETX INC.'S NOTICE OF COMPLIANCE WITH P.R. 3-1 AND P.R. 3-2 (Cawley, Douglas) (Entered: 02/14/2011)
- 02/15/2011 78 ORDER that parties are to submit agreed Docket Control and Discovery Orders to the Court by 2-28-2011. For purposes of computing the time deadlines under the local patent rules, the Court deems 2-28-2011 as the effective Rule 16 Initial Case Management Conference date, and thus plaintiff's PR 3-1 and 3-2 disclosures will be due 2-18-2011. Signed by Judge Leonard Davis on 02/15/11. cc:attys 2-15-11(ml,) (Entered: 02/15/2011)
- 02/16/2011 79 Unopposed MOTION FOR EXTENSION OF TIME TO ANSWER OR OTHERWISE RESPOND TO PLAINTIFF VIRNETX INC.S FIRST AMENDED COMPLAINT by Apple Inc.. (Attachments: # 1 Text of Proposed Order)(Williams, Danny) (Entered: 02/16/2011)
- 02/16/2011 80 Agreed MOTION for Extension of Time to File Answer to Plaintiff's First Amended Complaint by Aastra Technologies Ltd., Aastra USA, Inc.. (Attachments: # 1 Text of Proposed Order)(Hyland, Jon) (Entered: 02/16/2011)
- 02/17/2011 81 ORDER granting 79 Motion for Extension of Time. Apple Inc shall have to 3-14-2011 to answer or otherwise respond to pltf's First Amended Complaint. Signed by Judge Leonard Davis on 02/17/11. cc:attys 2-17-11 (ml,) (Entered: 02/17/2011)
- 02/17/2011 82 ORDER granting 80 Motion for Extension of Time to Answer. Aastra USA Inc and Aastra Technologies Ltd shall have to 3-10-2011 to answer, move, or otherwise respond to pltf's First Amended Complaint. Signed by Judge Leonard Davis on 02/17/11. cc:attys 2-17-11 (ml,) (Entered: 02/17/2011)
- 02/17/2011 83 Unopposed MOTION for Extension of Time to File Answer re 75 Amended Complaint, or Otherwise Respond by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Findlay, Eric) (Entered: 02/17/2011)
- 02/18/2011 84 Unopposed MOTION for Extension of Time to File Answer or Otherwise Respond by NEC Corporation, NEC Corporation of America. (Attachments: # 1 Text of Proposed Order)(McSwane, Douglas) (Entered: 02/18/2011)
- 02/22/2011 85 ORDER granting 83 Motion for Extension of Time to Answer. Deft Cisco Systems Inc shall have to 3-14-2011 to answer, move or otherwise respond to pltf's First Amended Complaint. Signed by Judge Leonard Davis on 02/22/11. cc:attys 2-22-11 (ml,) (Entered: 02/22/2011)
- 02/22/2011 86 ORDER granting 84 Motion for Extension of Time to Answer. Defts NEC Corporation and NEC Corporation of America shall have to 3-14-2011 to answer, move, or otherwise respond to pltf's Amended Complaint. Signed by Judge Leonard Davis on 02/22/11. cc:attys 2-23-11 (ml,) (Entered: 02/23/2011)
- 02/28/2011 87 Unopposed MOTION for Extension of Time to File PROPOSED DOCKET CONTROL AND DISCOVERY ORDERS by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America. (Attachments: # 1 Text of Proposed Order)(Williams, Danny) (Entered: 02/28/2011)
- 03/03/2011 88 Joint MOTION FOR ENTRY OF DOCKET CONTROL AND DISCOVERY ORDERS by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Proposed Docket Control Order, # 4 Proposed Discovery Order)(Cawley, Douglas) (Entered: 03/03/2011)
- 03/10/2011 89 Aastra USA Inc.'s ANSWER to 75 Amended Complaint,, COUNTERCLAIM against VirnetX Inc. by Aastra USA, Inc..(Hyland, Jon) (Entered: 03/10/2011)
- 03/10/2011 90 Aastra Technologies Limited's ANSWER to 75 Amended Complaint,, COUNTERCLAIM against VirnetX Inc. by Aastra Technologies Ltd..(Hyland, Jon) (Entered: 03/10/2011)

- 03/13/2011 91 NEC Corporation & NEC Corporation of America's First Amended ANSWER to 75 Amended Complaint,, COUNTERCLAIM against VirnetX Inc. by NEC Corporation of America, NEC Corporation.(McSwane, Douglas) (Entered: 03/13/2011)
- 03/14/2011 92 ANSWER to 75 Amended Complaint,, COUNTERCLAIM (DEFENDANT APPLE INC.S ORIGINAL ANSWER, AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS TO PLAINTIFFS FIRST AMENDED COMPLAINT) against VirnetX Inc. by Apple Inc..(Williams, Danny) (Entered: 03/14/2011)
- 03/14/2011 93 ANSWER to 75 Amended Complaint, Affirmative Defenses , COUNTERCLAIM against VirnetX Inc. by Cisco Systems, Inc..(Findlay, Eric) (Entered: 03/14/2011)
- 03/22/2011 94 APPLICATION to Appear Pro Hac Vice by Attorney Karim Z Oussayef for Cisco Systems, Inc. (mll,) (Entered: 03/22/2011)
- 03/25/2011 95 NOTICE by VirnetX Inc. JOINT NOTICE REGARDING MEDIATION (Cawley, Douglas) (Entered: 03/25/2011)
- 03/30/2011 96 NOTICE by Cisco Systems, Inc. Notice of Service of Initial Disclosures (Findlay, Eric) (Entered: 03/30/2011)
- 03/30/2011 97 NOTICE by Apple Inc. OF COMPLIANCE regarding Initial Disclosures (Williams, Danny) (Entered: 03/30/2011)
- 03/30/2011 98 NOTICE by NEC Corporation, NEC Corporation of America Notice of Compliance (McSwane, Douglas) (Entered: 03/30/2011)
- 03/30/2011 99 NOTICE of Disclosure by VirnetX Inc. (Cawley, Douglas) (Entered: 03/30/2011)
- 03/31/2011 100 NOTICE of Disclosure by Aastra Technologies Ltd., Aastra USA, Inc. of Initial Disclosures (Hyland, Jon) (Entered: 03/31/2011)
- 04/04/2011 101 ANSWER to 90 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 04/04/2011)
- 04/04/2011 102 ANSWER to 89 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 04/04/2011)
- 04/04/2011 103 ANSWER to 92 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 04/04/2011)
- 04/04/2011 104 ANSWER to 91 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 04/04/2011)
- 04/04/2011 105 ANSWER to 93 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 04/04/2011)
- 04/05/2011 106 MOTION for Leave to File SECOND AMENDED COMPLAINT by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 04/05/2011)
- 04/05/2011 107 AMENDED COMPLAINT against Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America, filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Exhibit E)(Cawley, Douglas) (Entered: 04/05/2011)
- 04/11/2011 108 ORDER granting 87 Motion for Extension of Time. The Court extends the deadlines for the parties to submit proposed docket control and discovery orders to 3-03-2011. Signed by Judge Leonard Davis on 04/11/11. cc:attys 4-11-11 (mll,) (Entered: 04/11/2011)
- 04/18/2011 109 NOTICE of Disclosure by Cisco Systems, Inc. Notice of Service of First Amended Initial Disclosures (Findlay, Eric) (Entered: 04/18/2011)
- 04/19/2011 110 DISCOVERY ORDER. Signed by Judge Leonard Davis on 04/19/11. cc:attys 4-20-11(mll,) (Entered: 04/20/2011)
- 04/19/2011 111 DOCKET CONTROL ORDER. Signed by Judge Leonard Davis on 04/19/11. cc:attys 4-20-11(mll,) (Entered: 04/20/2011)
- 04/19/2011 -- Deadlines set per 111 Docket Control Order: Amended Pleadings due by 9/28/2011; Respond to Amended Pleadings by 10-12-2011. Fact Discovery due by 4/13/2012; Expert Discovery due by 6-29-2012. Expert Witness List due by 4/27/2012; Rebuttal Expert Witnesses designated by 6-01-2012.

- Identify trial witnesses by 6/29/2012; Rebuttal Trial Witnesses identified by 7-10-2012. Joinder of Parties due by 6/17/2011, for deft. Jury instructions due by 8/24/2012. Mediation Completion due by 12/31/2011. Dispositive Motions due by 7/13/2012; Response to Dispositive Motions due 8-17-2012. Proposed Pretrial Order due by 8/24/2012. Motions in Limine due 9-28-2012; Responses to Motions in Limine due 10-05-2012. Jury Selection set for 11/5/2012 09:00AM before Judge Leonard Davis. Jury Trial set for 11/13/2012 09:00 AM before Judge Leonard Davis. Markman Hearing set for 1/5/2012 09:00 AM before Judge Leonard Davis. Pretrial Conference set for 10/18/2012 09:00 AM before Judge Leonard Davis. Estimated length of trial is 5-7 days. (mll,) (Entered: 04/21/2011)
- 04/21/2011 112 Unopposed MOTION for Extension of Time to Complete Discovery, Unopposed MOTION for Extension of Time to File Response/Reply as to 106 MOTION for Leave to File SECOND AMENDED COMPLAINT [(UNOPPOSED MOTION FOR EXTENSION OF TIME FOR DEFENDANTS TO FILE THEIR RESPONSE TO PLAINTIFF VIRNETX INC.S MOTION FOR LEAVE TO AMEND ITS COMPLAINT AND ITS INFRINGEMENT CONTENTIONS)] by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America. (Attachments: # 1 Text of Proposed Order)(Williams, Danny) (Entered: 04/21/2011)
- 04/27/2011 113 ORDER granting 112 Motion for Extension of Time to Complete Discovery; granting 112 Motion for Extension of Time to File Response/Reply re 106 MOTION for Leave to File SECOND AMENDED COMPLAINT ; Responses due by 4/29/2011. Signed by Judge Leonard Davis on 04/27/11. cc:attys 4-27-11 (mll,) (Entered: 04/27/2011)
- 04/29/2011 114 NOTICE by VirnetX Inc. re 106 MOTION for Leave to File SECOND AMENDED COMPLAINT (JOINT NOTICE REGARDING DEFENDANTS' NON-OPPOSITION TO PLAINTIFF'S MOTION FOR LEAVE TO AMEND) (Cawley, Douglas) (Entered: 04/29/2011)
- 04/29/2011 115 Unopposed MOTION to Amend/Correct THE DISCOVERY ORDER AND DOCKET CONTROL ORDER by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America. (Attachments: # 1 Text of Proposed Order)(Williams, Danny) (Entered: 04/29/2011)
- 05/02/2011 116 ORDER granting 106 Motion for Leave to Amend Complaint. Signed by Judge Leonard Davis on 05/02/11. cc:attys 5-03-11 (mll,) (Entered: 05/03/2011)
- 05/02/2011 117 ORDER granting 115 Motion to Amend/Correct Discovery Order and Docket Control Order. Signed by Judge Leonard Davis on 05/02/11. cc:attys 5-03-11 (mll,) (Entered: 05/03/2011)
- 05/03/2011 118 NOTICE by VirnetX Inc. re 116 Order on Motion for Leave to File (Cawley, Douglas) (Entered: 05/03/2011)
- 05/17/2011 119 Unopposed MOTION to Withdraw as Attorney by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order Proposed Order)(Hamill, Andrew) (Entered: 05/17/2011)
- 05/20/2011 120 Joint MOTION to Dismiss with Prejudice for Virnetx' Intentional Failure to Secure Standing to Bring Suit by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America. (Attachments: # 1 Declaration of M. Stadnick, # 2 Exhibit A - April 18th email, # 3 Exhibit B - April 20th email, # 4 Text of Proposed Order)(Jones, Michael) (Entered: 05/20/2011)
- 05/23/2011 121 Aastra USA Inc.'s ANSWER to 107 Amended Complaint, Affirmative Defenses , COUNTERCLAIM against VirnetX Inc. by Aastra USA, Inc..(Hyland, Jon) (Entered: 05/23/2011)
- 05/23/2011 122 Aastra Technologies Limited's ANSWER to 107 Amended Complaint, Affirmative Defenses , COUNTERCLAIM against VirnetX Inc. by Aastra Technologies Ltd..(Hyland, Jon) (Entered: 05/23/2011)
- 05/24/2011 123 NOTICE of Attorney Appearance by John Austin Curry on behalf of VirnetX Inc. (Curry, John) (Entered: 05/24/2011)
- 05/26/2011 124 ORDER granting 119 Motion to Withdraw as Attorney. Attorney Andrew G Hamill terminated. Signed by Judge Leonard Davis on 05/26/11. cc:attys 5-26-11 (mll,) (Entered: 05/26/2011)

- 05/31/2011 125 ORDER REFERRING CASE to Mediator. Robert Faulkner added as Mediator. Signed by Judge Leonard Davis on 05/31/11. cc:attys 5-31-11(ml,) (Entered: 05/31/2011)
- 06/03/2011 126 NOTICE of Attorney Appearance by Peter Chang on behalf of Cisco Systems, Inc. (Chang, Peter) (Entered: 06/03/2011)
- 06/06/2011 127 Unopposed MOTION to Seal PLAINTIFF'S RESPONSE TO DEFENDANTS' MOTION TO DISMISS by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 06/06/2011)
- 06/06/2011 128 SEALED PATENT RESPONSE to SEALED PATENT MOTION re 120 Joint MOTION to Dismiss with Prejudice for Virnetx' Intentional Failure to Secure Standing to Bring Suit filed by VirnetX Inc. . (Attachments: # 1 Declaration Sameer Mather, # 2 Exhibit A, # 3 Exhibit B, # 4 Exhibit C, # 5 Exhibit D, # 6 Exhibit E, # 7 Text of Proposed Order, # 8 Alternative Proposed Order)(Cawley, Douglas) (Entered: 06/06/2011)
- 06/06/2011 129 MOTION for Leave to File An Opposition to Defendants' Motion to Dismiss by Science Applications International Corporation. (Attachments: # 1 Exhibit SAIC's Opposition to Motion to Dismiss, # 2 Affidavit Declaration of Andy Tindel, # 3 Exhibit A to Tindel Declaration, # 4 Text of Proposed Order) (Tindel, Andy) (Entered: 06/06/2011)
- 06/08/2011 130 ORDER granting 127 Motion to Seal Pltf's Response to Defts' Motion to Dismiss. Signed by Judge Leonard Davis on 06/08/11. cc:attys 6-08-11 (ml,) (Entered: 06/08/2011)
- 06/08/2011 131 ANSWER to 121 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 06/08/2011)
- 06/08/2011 132 ANSWER to 122 Answer to Amended Complaint, Counterclaim by VirnetX Inc.. (Cawley, Douglas) (Entered: 06/08/2011)
- 06/09/2011 133 RESPONSE in Opposition re 120 Joint MOTION to Dismiss with Prejudice for Virnetx' Intentional Failure to Secure Standing to Bring Suit filed by Science Applications International Corporation . (Attachments: # 1 Affidavit Declaration of Andy Tindel, # 2 Exhibit A to Declaration of Andy Tindel, # 3 Text of Proposed Order)(Tindel, Andy) (Entered: 06/09/2011)
- 06/16/2011 134 Unopposed MOTION to Seal Their Reply Brief in Support of Defendants' Motion to Dismiss by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America. (Attachments: # 1 Text of Proposed Order)(Jones, Michael) (Entered: 06/16/2011)
- 06/16/2011 135 SEALED PATENT REPLY to Response to PATENT Motion re 120 Joint MOTION to Dismiss with Prejudice for Virnetx' Intentional Failure to Secure Standing to Bring Suit filed by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America . (Jones, Michael) (Entered: 06/16/2011)
- 06/16/2011 136 RESPONSE to Motion re 129 MOTION for Leave to File An Opposition to Defendants' Motion to Dismiss filed by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America . (Attachments: # 1 Text of Proposed Order)(Jones, Michael) (Entered: 06/16/2011)
- 06/20/2011 137 ORDER granting 134 Motion to Seal. Signed by Judge Leonard Davis on 6/20/2011. (gsg) (Entered: 06/20/2011)
- 06/27/2011 138 Unopposed MOTION to Seal PLAINTIFF'S SURREPLY TO DEFENDANTS' MOTION T DISMISS by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order) (Cawley, Douglas) (Entered: 06/27/2011)
- 06/27/2011 139 SEALED PATENT SUR-REPLY to Reply to Response to PATENT Motion re 120 Joint MOTION to Dismiss with Prejudice for Virnetx' Intentional Failure to Secure Standing to Bring Suit filed by VirnetX Inc. . (Cawley, Douglas) (Entered: 06/27/2011)
- 06/27/2011 140 REPLY to Response to Motion re 129 MOTION for Leave to File An Opposition to Defendants' Motion to Dismiss SAIC's Reply to Defendants' Response to SAIC's Motion for Leaved to File Opposition to Defendants' Motion to Dismiss with Prejudice for VirnetX' Failure to Secure Standing to Bring Suit filed by Science Applications International Corporation . (Tindel, Andy) (Entered: 06/27/2011)

- 06/29/2011 141 ORDER granting 138 Motion to Seal Plt's Surreply to Defts' Motion to Dismiss. Signed by Judge Leonard Davis on 06/29/11. cc:attys 6-30-11 (mll,) (Entered: 06/30/2011)
- 07/05/2011 142 NOTICE by Cisco Systems, Inc. Notice of Service of Second Amended Initial Disclosures (Findlay, Eric) (Entered: 07/05/2011)
- 07/07/2011 143 SUR-REPLY to Reply to Response to Motion re 129 MOTION for Leave to File An Opposition to Defendants' Motion to Dismiss filed by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America . (Jones, Michael) (Entered: 07/07/2011)
- 07/25/2011 144 NOTICE by NEC Corporation, NEC Corporation of America (Notice of Firm Name Change) (McSwane, Douglas) (Entered: 07/25/2011)
- 07/29/2011 145 Joint MOTION for Protective Order by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 07/29/2011)
- 08/02/2011 146 AGREED PROTECTIVE ORDER. Signed by Judge Leonard Davis on 08/02/11. cc:attys 8-02-11(mll,) (Entered: 08/02/2011)
- 08/09/2011 147 Unopposed MOTION to Withdraw as Attorney (Phillip N. Cockrell) by Aastra Technologies Ltd., Aastra USA, Inc.. (Attachments: # 1 Text of Proposed Order)(Hyland, Jon) (Entered: 08/09/2011)
- 08/11/2011 148 ORDER granting 147 Motion to Withdraw as Attorney. Attorney Phillip Nollin Cockrell terminated. Signed by Judge Leonard Davis on 08/11/11. cc:attys 08/11/11 (mll,) (Entered: 08/11/2011)
- 08/29/2011 149 NOTICE by Apple Inc. OF COMPLIANCE (Williams, Danny) (Entered: 08/29/2011)
- 08/30/2011 150 NOTICE by NEC Corporation, NEC Corporation of America of Compliance of service of Supplemental Disclosures (McSwane, Douglas) (Entered: 08/30/2011)
- 09/14/2011 151 Unopposed MOTION for Extension of Time to File Motion Seeking Relief from the Court under Paragraph 12(b) of the Agreed Protective Order Regarding the Disclosure of William C. Easttom by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Findlay, Eric) (Entered: 09/14/2011)
- 09/15/2011 152 ORDER granting 151 Motion for Extension of Time. The deadline for defendantsto seek relief from the Court regarding objections to Mr. William C Easttom lodged properly under the Protective Order shall be extended through 9-19-2011. Signed by Judge Leonard Davis on 09/15/11. cc:attys 9-15-11 (mll,) (Entered: 09/15/2011)
- 09/19/2011 153 Unopposed MOTION for Extension of Time to File Defendants' Motion Seeking Relief From The Court Under Paragraph 12(b) of the Agreed Protective Order Regarding the Disclosure of William C. Easttom by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Findlay, Eric) (Entered: 09/19/2011)
- 09/20/2011 154 ORDER granting 153 Motion for Extension of Time. The deadline for Defendants to seek relief from the Court regarding objections to Mr. Easttom lodged properly under the Protective Order shall be extended through 9-26-2011. Signed by Judge Leonard Davis on 09/20/11. cc:attys 9-20-11 (mll,) (Entered: 09/20/2011)
- 09/20/2011 155 NOTICE of Attorney Appearance by Ramzi Ragheb Khazen on behalf of VirnetX Inc. (Khazen, Ramzi) (Entered: 09/20/2011)
- 09/26/2011 156 Joint MOTION for Extension of Time for the Parties to Provide the Court with Technology Tutorials by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America, VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Jones, Michael) (Entered: 09/26/2011)
- 09/28/2011 157 ORDER granting 156 Motion for Extension of Time. The deadline for parties to provide the Court with technology tutorials shall be extended to 11-10-2011. Signed by Judge Leonard Davis on 09/28/11. cc:attys 9-28-11 (mll,) (Entered: 09/28/2011)
- 09/28/2011 158 Unopposed MOTION to Amend/Correct 117 Order on Motion to Amend/Correct by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 09/28/2011)

- 09/29/2011 159 ORDER granting 158 Motion to Amend/Correct. The deadline set forth in theOrder Granting Defendants Motion to Amend the Discovery Order and Docket Control Order 117 shall be extended to 10-04-2011. Signed by Judge Leonard Davis on 09/29/11. cc:attys 9-29-11 (mll,) (Entered: 09/29/2011)
- 10/04/2011 160 Unopposed MOTION to Amend/Correct 159 Order on Motion to Amend/Correct, by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 10/04/2011)
- 10/05/2011 161 ORDER granting 160 Motion for Leave to Extend the Deadline for filing the Joint Claim Construction and Prehearing Statement. Deadline is extended to 10/11/2011. Signed by Judge Leonard Davis on 10/5/11. (mjc,) (Entered: 10/05/2011)
- 10/05/2011 162 PLEASE IGNORE. Atty filed pleading in wrong case. PLEASE IGNORE. . NOTICE of Attorney Appearance by John Austin Curry on behalf of VirnetX Inc. (Curry, John) Modified on 10/6/2011 (leh,). (Entered: 10/05/2011)
- 10/07/2011 163 NOTICE of Attorney Appearance by Matthew Richard Rodgers on behalf of Apple Inc. (Rodgers, Matthew) (Entered: 10/07/2011)
- 10/11/2011 164 JOINT CLAIM CONSTRUCTION AND PREHEARING STATEMENT filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D) (Cawley, Douglas) (Entered: 10/11/2011)
- 10/19/2011 165 Unopposed MOTION for Extension of Time to Serve Privilege Logs by Cisco Systems, Inc.. (Attachments: # 1 Text of Proposed Order)(Findlay, Eric) (Entered: 10/19/2011)
- 10/20/2011 166 ORDER granting 165 Motion for Extension of Time. Parties shall have to 10-31-2011 to serve privilege logs. Signed by Judge Leonard Davis on 10/20/11. cc:attys 10-20-11 (mll,) (Entered: 10/20/2011)
- 10/28/2011 167 Joint MOTION to Amend/Correct 117 Order on Motion to Amend/Correct by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 10/28/2011)
- 10/31/2011 168 ORDER granting 167 Motion to Amend/Correct Docket Control Order and extending deadlines to file briefs. Signed by Judge Leonard Davis on 10/31/11. cc:attys 10-31-11 (mll,) (Entered: 10/31/2011)
- 10/31/2011 169 Unopposed MOTION for Extension of Time to File Privilege Logs by NEC Corporation, NEC Corporation of America. (Attachments: # 1 Text of Proposed Order)(McSwane, Douglas) (Entered: 10/31/2011)
- 11/01/2011 170 Joint MOTION for Leave to File Excess Pages by VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Cawley, Douglas) (Entered: 11/01/2011)
- 11/01/2011 171 ORDER granting 169 Motion for Extension of Time. NEC defts shall have to 11-07-2011 to serve privilege logs. Signed by Judge Leonard Davis on 11/01/11. cc:attys 11-01-11 (mll,) (Entered: 11/01/2011)
- 11/03/2011 172 ORDER denying 170 Motion for Leave to File Excess Pages. Parties are ordered to meet and confer and narrow the number of disputed terms to a reasonable number, and to file an amended P.R. 4-3 Statement by 11-07-2011. Signed by Judge Leonard Davis on 11/03/11. cc:attys 11-03-11 (mll,) (Entered: 11/03/2011)
- 11/04/2011 173 OPENING CLAIM CONSTRUCTION BRIEF filed by VirnetX Inc.. (Attachments: # 1 Declaration of Austin Curry, # 2 Exhibit 1, # 3 Exhibit 2, # 4 Exhibit 3, # 5 Exhibit 4, # 6 Exhibit 5, # 7 Exhibit 6, # 8 Exhibit A, # 9 Exhibit B, # 10 Exhibit C, # 11 Exhibit D, # 12 Exhibit E, # 13 Exhibit F, # 14 Exhibit G, # 15 Exhibit H, # 16 Exhibit I, # 17 Declaration of Mark T. Jones)(Cawley, Douglas) (Entered: 11/05/2011)
- 11/07/2011 174 ***FILED IN ERROR. SEE DOCUMENT 175 FOR CORRECT PLEADING*** JOINT CLAIM CONSTRUCTION AND PREHEARING STATEMENT filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D) (Cawley, Douglas) Modified on 11/8/2011 (mll,). (Entered: 11/07/2011)
- 11/08/2011 175 JOINT CLAIM CONSTRUCTION AND PREHEARING STATEMENT filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D) (Cawley, Douglas) (Entered: 11/08/2011)
- 11/09/2011 176 NOTICE by NEC Corporation, NEC Corporation of America of Compliance and Privilege Log (McSwane, Douglas) (Entered: 11/09/2011)

- 11/17/2011 177 NOTICE by Cisco Systems, Inc. of Disclosure Regarding Technology Tutorial (Findlay, Eric) (Entered: 11/17/2011)
- 11/18/2011 178 NOTICE by VirnetX Inc. NOTICE OF COMPLIANCE WITH P.R. 3-1 AND 3-2 AND ORDER DATED MAY 2, 2011 (Cawley, Douglas) (Entered: 11/18/2011)
- 11/18/2011 179 SEALED PATENT MOTION TO COMPEL FROM APPLE A COMPLETE RESPONSE TO VIRNETX'S EIGHTH COMMON INTERROGATORY by VirnetX Inc.. (Attachments: # 1 Exhibit A.1, # 2 Exhibit A.2, # 3 Exhibit A.3, # 4 Exhibit A.4, # 5 Exhibit A.5, # 6 Exhibit A.6, # 7 Text of Proposed Order)(Cawley, Douglas) (Entered: 11/18/2011)
- 11/30/2011 180 NOTICE of Attorney Appearance by Mitchell Reed Sibley on behalf of VirnetX Inc. (Sibley, Mitchell) (Entered: 11/30/2011)
- 12/02/2011 181 NOTICE by Cisco Systems, Inc. of Third-Party Discovery (Attachments: # 1 Exhibit 1 - Subpoena)(Findlay, Eric) (Entered: 12/02/2011)
- 12/07/2011 182 DEFENDANTS' RESPONSIVE CLAIM CONSTRUCTION BRIEF filed by Aastra Technologies Ltd., Aastra USA, Inc., Apple Inc., Cisco Systems, Inc., NEC Corporation, NEC Corporation of America. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7, # 8 Exhibit A, # 9 Exhibit B, # 10 Exhibit C, # 11 Exhibit D, # 12 Exhibit E, # 13 Exhibit F, # 14 Exhibit G, # 15 Exhibit H, # 16 Exhibit I, # 17 Exhibit J, # 18 Exhibit K, # 19 Exhibit L, # 20 Exhibit M, # 21 Exhibit N, # 22 Exhibit O, # 23 Exhibit P)(Kheyfits, Dmitriy) (Entered: 12/07/2011)
- 12/08/2011 183 Additional Attachments to Main Document: 182 Claim Construction Brief,... (Attachments: # 1 Affidavit DECLARATION OF JOHN P. J. KELLY, Ph.D.) (Kheyfits, Dmitriy) (Entered: 12/08/2011)
- 12/08/2011 184 Unopposed MOTION for Extension of Time to File Response/Reply as to 179 SEALED PATENT MOTION TO COMPEL FROM APPLE A COMPLETE RESPONSE TO VIRNETX'S EIGHTH COMMON INTERROGATORY by Apple Inc.. (Attachments: # 1 Text of Proposed Order)(Williams, Danny) (Entered: 12/08/2011)
- 12/09/2011 185 ORDER granting 184 Motion for Extension of Time to File Response/Reply re 179 SEALED PATENT MOTION TO COMPEL FROM APPLE A COMPLETE RESPONSE TO VIRNETX'S EIGHTH COMMON INTERROGATORY ; Responses due by 12/15/2011. Signed by Judge Leonard Davis on 12/09/11. cc:attys 12-09-11 (mll,) (Entered: 12/09/2011)
- 12/13/2011 186 NOTICE of Attorney Appearance by Eric Miller Albritton on behalf of Apple Inc. (Albritton, Eric) (Entered: 12/13/2011)
- 12/14/2011 187 NOTICE by VirnetX Inc. NOTICE OF ESTIMATED AMOUNT OF TIME REQUESTED FOR THE MARKMAN HEARING (Cawley, Douglas) (Entered: 12/14/2011) Events

since last

full&nbsupdate

Copyright © 2011 LexisNexis CourtLink, Inc. All rights reserved.
 *** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***

US District Court Civil Docket

**U.S. District - Texas Eastern
(Tyler)**

6:10cv94

Virnetx Inc v. Microsoft Corporation

This case was retrieved from the court on Wednesday, December 14, 2011

Date Filed: 03/17/2010 **Class Code: CLOSED**
Assigned To: Judge Leonard Davis **Closed: Yes**
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

Bradley Wayne Caldwell
[COR LD NTC]
McKool Smith
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4000
Fax: 2149784044
Email: Bcaldwell@mckoolsmith.com

Jason Dodd Cassady
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: Jcassady@mckoolsmith.com

Luke Fleming McLeroy
[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214-978-4000
Fax: 214-978-4044
Email: LMCLEROY@MCKOOLSMITH.COM

Douglas A Cawley

Microsoft Corporation
Defendant

[COR LD NTC]
McKool Smith -Dallas
300 Crescent Court
Suite 1500
Dallas , TX 75201
USA
214/ 978-4972
Fax: 12149784044
Email: Dcawley@mckoolsmith.com

Matthew Douglas Powers
[COR LD NTC]
Tensegrity Law Group, LLP
201 Redwood Shores Parkway
Suite 401
Redwood Shores , CA 94065
USA
650-802-6000
Fax: 650-802-6001
Email:
MATTHEW.POWERS@TENSEGRITYLAWGROUP.COM

Amber Hatfield Rovner
[COR LD NTC]
Weil Gotshal & Manges-Houston
700 Louisiana
Suite 1600
Houston , TX 77002-2784
USA
201-386-2955
Fax: 713-223-9511
Email: AMBER.ROVNER@WEIL.COM

Daniel James Booth
[COR LD NTC]
Weil Gotshal & Manges-Houston
700 Louisiana
Suite 1600
Houston , TX 77002-2784
USA
713-546-5135
Fax: 713-224-9511

Elizabeth S Weiswasser
[COR LD NTC]
Weil Gotshal & Manges-NY
767 Fifth Avenue
New York , NY 10153-0119
USA
212-310-8022
Fax: 212-310-8007
<i>pro Hac Vice</ I>
Email: ELIZABETH.WEISWASSER@WEIL.COM

Eric Hugh Findlay
[COR LD NTC]
Findlay Craft
6760 Old Jacksonville Hwy
Suite 101
Tyler , TX 75703
USA
903/ 534-1100
Fax: 903/ 534-1137
Email: EFINDLAY@FINDLAYCRAFT.COM

Jared B Bobrow

[COR LD NTC]
 Weil Gotshal & Manges-Redwood Shores
 201 Redwood Shores Parkway
 5TH Floor
 Redwood City , CA 94065
 USA
 605/ 802-3034
 Fax: 605/ 802-3100
 <i>pro Hac Vice</ I>
 Email: JARED.BOBROW@WEIL.COM

Paul T Ehrlich
 [COR LD NTC]
 Tensegrity Law Group, LLP
 201 Redwood Shores Parkway
 Suite 401
 Redwood Shores , CA 94065
 USA
 650/ 802-6000
 Fax: 650/ 802-6001
 Email: PAUL.EHRLICH@TENSEGRITYLAWGROUP.COM

Robert Lewis Gerrity
 [COR LD NTC]
 Tensegrity Law Group, LLP
 201 Redwood Shores Parkway
 Suite 401
 Redwood Shores , CA 94065
 USA
 650/ 802-6000
 Fax: 650/ 802-6001
 Email: ROBERT.GERRITY@TENSEGRITYLAWGROUP.COM

Roger Brian Craft
 [COR LD NTC]
 Findlay Craft
 6760 Old Jacksonville Hwy
 Suite 101
 Tyler , TX 75703
 USA
 903/ 534-1100
 Fax: 903/ 534-1137
 Email: BCRAFT@FINDLAYCRAFT.COM

Thomas B King
 [COR LD NTC]
 Thomas Whitelaw & Tyler LLP
 18101 Von Karman Avenue
 Suite 230
 Irvine , CA 92612
 USA
 949/ 679-6400
 Fax: 949/ 679-6405
 Email: TKING@TWTLAW.COM

Date	#	Proceeding Text	Source
03/17/2010	1	COMPLAINT against Microsoft Corporation (Filing fee \$ 350 receipt number 0540-2403564.), filed by VirnetX Inc.. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Civil Cover Sheet)(Cawley, Douglas) (Entered: 03/17/2010)	
03/17/2010	2	CORPORATE DISCLOSURE STATEMENT filed by VirnetX Inc. identifying Corporate Parent None for VirnetX Inc.. (Cawley, Douglas) (Entered: 03/17/2010)	
03/17/2010	--	Judge Leonard Davis added. (mll,) (Entered: 03/18/2010)	
03/22/2010	3	E-GOV SEALED SUMMONS Issued as to Microsoft Corporation, and emailed to pltf for service. (mll,) (Entered: 03/22/2010)	

- 03/24/2010 4 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint Agreed Motion for Extension of Time to Answer, Move, or Otherwise Respond to Plaintiff's Complaint by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Findlay, Eric) (Entered: 03/24/2010)
- 03/25/2010 5 ORDER granting 4 Motion for Extension of Time to Answer. Microsoft shall answer, move, or otherwise respond to pltf's Complaint by 5-10-2010. Signed by Judge Leonard Davis on 03/25/10. cc:attys 3-25-10 (mll,) (Entered: 03/25/2010)
- 03/26/2010 6 CORPORATE DISCLOSURE STATEMENT filed by Microsoft Corporation identifying Corporate Parent None for Microsoft Corporation. (Findlay, Eric) (Entered: 03/26/2010)
- 03/30/2010 7 NOTICE of Attorney Appearance by Luke Fleming McLeroy on behalf of VirnetX Inc. (McLeroy, Luke) (Entered: 03/30/2010)
- 03/30/2010 8 NOTICE of Attorney Appearance by Jason Dodd Cassidy on behalf of VirnetX Inc. (Cassady, Jason) (Entered: 03/30/2010)
- 03/30/2010 9 NOTICE of Attorney Appearance by Bradley Wayne Caldwell on behalf of VirnetX Inc. (Caldwell, Bradley) (Entered: 03/30/2010)
- 04/21/2010 10 NOTICE of Attorney Appearance by Roger Brian Craft on behalf of Microsoft Corporation (Craft, Roger) (Entered: 04/21/2010)
- 04/26/2010 11 ORDER that plaintiff file a notice that the case is ready for scheduling conference when all of the defendants have either answered or filed a motion to transfer or dismiss. The notice shall be filed within five days of the last remaining defendant's answer or motion. Signed by Judge Leonard Davis on 04/26/10. cc:attys 4-27-10(mll,) (Entered: 04/27/2010)
- 05/05/2010 12 NOTICE of Attorney Appearance by Matthew Douglas Powers on behalf of Microsoft Corporation (Powers, Matthew) (Entered: 05/05/2010)
- 05/05/2010 13 NOTICE of Attorney Appearance by Daniel James Booth on behalf of Microsoft Corporation (Booth, Daniel) (Entered: 05/05/2010)
- 05/05/2010 14 NOTICE of Attorney Appearance by Paul T Ehrlich on behalf of Microsoft Corporation (Ehrlich, Paul) (Entered: 05/05/2010)
- 05/05/2010 15 NOTICE of Attorney Appearance by Amber Hatfield Rovner on behalf of Microsoft Corporation (Rovner, Amber) (Entered: 05/05/2010)
- 05/06/2010 16 APPLICATION to Appear Pro Hac Vice by Attorney Jared B Bobrow for Microsoft Corporation. (mll,) (Entered: 05/06/2010)
- 05/06/2010 17 APPLICATION to Appear Pro Hac Vice by Attorney Robert Lewis Gerrity for Microsoft Corporation. (mll,) (Entered: 05/06/2010)
- 05/06/2010 18 APPLICATION to Appear Pro Hac Vice by Attorney Thomas B King for Microsoft Corporation. (mll,) (Entered: 05/06/2010)
- 05/06/2010 19 APPLICATION to Appear Pro Hac Vice by Attorney Elizabeth S Weiswasser for Microsoft Corporation. (mll,) (Entered: 05/06/2010)
- 05/07/2010 20 Unopposed MOTION for Extension of Time to File Answer re 1 Complaint Second Agreed Motion for Extension of Time to Answer, Move, or Otherwise Respond to Plaintiff's Complaint by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Booth, Daniel) (Entered: 05/07/2010)
- 05/07/2010 21 ORDER granting 20 Motion for Extension of Time to Answer. Microsoft shall answer, move, or otherwise respond to pltf's Complaint by 5-24-2010. Signed by Judge Leonard Davis on 05/07/10. cc:attys 5-07-10 (mll,) (Entered: 05/07/2010)
- 05/18/2010 22 STIPULATION of Dismissal by Microsoft Corporation, VirnetX Inc.. (Attachments: # 1 Text of Proposed Order)(Powers, Matthew) (Entered: 05/18/2010)
- 05/25/2010 23 ORDER granting 22 Stipulation of Dismissal filed by VirnetX Inc., Microsoft Corporation. All of the claims asserted against Microsoft in this action are dismissed with prejudice. Each party shall bear its own costs, expenses and fees. This is a Final Judgment. Signed by Judge Leonard Davis on 05/24/10. cc:attys 5-25-10(mll,) (Entered: 05/25/2010)

Copyright © 2011 LexisNexis CourtLink, Inc. All rights reserved.
*** THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY ***

1. 7,188,180, INTER PARTES REEXAMINATION CERTIFICATE C1 (0274th), Jun. 7, 2011, Method for Establishing Secure Communication Link Between Computers of Virtual Private Network, Larson, Victor, Fairfax, Virginia (US) Short, Robert Dunham III, Leesburg, Virginia (US) Munger, Edmund Colby, Crownsville, Maryland (US) Williamson, Michael, South Riding, Virginia (US), Virnetx Inc., Scotts Valley Drive, California (US)
2. 7188180, June 3, 2004, Method for establishing secure communication link between computers of virtual private network, Larson, Victor, Fairfax, VIRGINIA , United States of America(US); Short, III, Robert Durham, Leesburg, VIRGINIA , United States of America(US); Munger, Edmund Colby, Crownsville, MARYLAND, United States of America(US); Williamson, Michael, South Riding, VIRGINIA , United States of America (US); 702486, November 7, 2003, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., SCIENCE APPLICATIONS INTERNATIONAL CORPORATION 10260 CAMPUS POINT DRIVE SAN DIEGO CALIFORNIA 92121, reel-frame:014679/0947; January 10, 2007, ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS)., VIRNETX INC. 5615 SCOTTS VALLEY DRIVE, SUITE 110 SCOTTS VALLEY DRIVE CALIFORNIA 95066, reel-frame:018757/0326, VimetX, Inc., Scotts Valley, CALIFORNIA , United States of America(US), United States company or corporation



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


Source: **Legal > Area of Law - By Topic > Patent Law > Find Patents > Utility, Design and Plant Patents** [\[i\]](#)

Terms: **PATNO=7188180** (Suggest Terms for My Search)

View: Cite

Date/Time: Wednesday, December 14, 2011 - 6:23 PM EST

-  1. VirnetX, Inc. v. Microsoft Corp., CASE NO. 6:07 CV 80, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, TYLER DIVISION, 2009 U.S. Dist. LEXIS 65667, July 30, 2009, Decided, July 30, 2009, Filed
- CORE TERMS:** network, domain, web, virtual, site, specification, server, user, target, proxy ...
-  2. VirnetX, Inc. v. Microsoft Corp., CASE NO. 6:07 CV 80, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, TYLER DIVISION, 2008 U.S. Dist. LEXIS 94854, June 3, 2008, Decided, June 4, 2008, Filed, Patent interpreted by VirnetX, Inc. v. Microsoft Corp., 2009 U.S. Dist. LEXIS 65667 (E.D. Tex., July 30, 2009)
- CORE TERMS:** patent-in-suit, patent, license, infringement, grantor, patent rights, substantial rights, grantee, joinder, join ...







Source: **Combined Source Set 3**  - **Intellectual Property Cases, Administrative Decisions & Regulations**

Terms: **7188180 or 7,188,180** (Suggest Terms for My Search)

View: Cite

Date/Time: Wednesday, December 14, 2011 - 6:24 PM EST

* Signal Legend:

-  - Warning: Negative treatment is indicated
 -  - Questioned: Validity questioned by citing refs
 -  - Caution: Possible negative treatment
 -  - Positive treatment is indicated
 -  - Citing Refs. With Analysis Available
 -  - Citation information available
- * Click on any *Shepard's* signal to *Shepardize*® that case.

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us
Copyright © 2011 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

1. Southeast Texas Record, August 18, 2010 Wednesday, 3277 words, Recent patent infringement/false marking suits filed in the Eastern District of Texas, Michelle Massey, East Texas Bureau
... Without User Entering Any Cryptographic Information, U.S. Patent No. **7,188,180** issued March 6, 2007, for Method for Establishing Secure Communication
...
2. 24/7 Wall St., August 12, 2010 Thursday 9:59 AM EST, , 396 words, Can VirnetX Win More Patent Suits? (VHC, AAPL, CSCO, MSFT), Administrator
The company noted the following patents as U.S. Patent Numbers: 6,502,135, 6,839,759, **7,188,180**, 7,418,504, 7,490,151. VirnetX did not specify in the release what it is asking for ...
3. Corporate IT Update, August 12, 2010 Thursday, 113 words, VirnetX files patent infringement lawsuit against multiple respondents
... NEC Corporation of America. The patents involved are US Patent Nos. 6,502,135, 6,839,759, **7,188,180**, 7,418,504 and 7,490,151. VirnetX said that it is seeking both damages and interactive relief.
4. Corporate IT Update, August 12, 2010 Thursday, 113 words, VirnetX files patent infringement lawsuit against multiple respondents
... NEC Corporation of America. The patents involved are US Patent Nos. 6,502,135, 6,839,759, **7,188,180**, 7,418,504 and 7,490,151. VirnetX said that it is seeking both damages and interactive relief.
5. Internet Business News, August 12, 2010 Thursday, 113 words, VirnetX files patent infringement lawsuit against multiple respondents
... NEC Corporation of America. The patents involved are US Patent Nos. 6,502,135, 6,839,759, **7,188,180**, 7,418,504 and 7,490,151. VirnetX said that it is seeking both damages and interactive relief.
6. PR Newswire, August 12, 2010 Thursday 8:00 AM EST, , 463 words, VirnetX Files New Lawsuit Against Multiple Companies; Apple, Cisco, NEC, and Aastra named in the complaint, SCOTTS VALLEY, Calif., Aug. 12
... five patents owned by VirnetX, U.S. Patent Nos. 6,502,135, 6,839,759, **7,188,180**, 7,418,504, 7,490,151. In its complaint, VirnetX seeks both damages and injunctive relief.
7. Telecomworldwire, August 12, 2010 Thursday, 119 words, VirnetX files patent infringement lawsuit against multiple respondents
... NEC Corporation of America. The patents involved are US Patent Nos. 6,502,135, 6,839,759, **7,188,180**, 7,418,504 and 7,490,151. VirnetX said that it is seeking both damages and interactive relief.
8. Telecomworldwire, August 12, 2010 Thursday, 113 words, VirnetX files patent infringement lawsuit against multiple respondents
... NEC Corporation of America. The patents involved are US Patent Nos. 6,502,135, 6,839,759, **7,188,180**, 7,418,504 and 7,490,151. VirnetX said that it is seeking both damages and interactive relief.
9. Briefing.com, June 22, 2010 Tuesday 11:00 PM EST, , 11500 words, Briefing.com: Hourly In Play (R) - 23:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...

10. Briefing.com, June 22, 2010 Tuesday 10:00 PM EST, , 11500 words, Briefing.com:
Hourly In Play (R) - 22:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...

Source: **Combined Source Set 3**  - **News, Most Recent Two Years (English, Full Text)**

Terms: **7188180 or 7,188,180** (Suggest Terms for My Search)

View: Cite

Date/Time: Wednesday, December 14, 2011 - 6:27 PM EST

In

[About LexisNexis](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Contact Us](#)
Copyright © 2011 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

11. Briefing.com, June 22, 2010 Tuesday 9:00 PM EST, , 11500 words, Briefing.com: Hourly In Play (R) - 21:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
12. Briefing.com, June 22, 2010 Tuesday 8:00 PM EST, , 11500 words, Briefing.com: Hourly In Play (R) - 20:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
13. Briefing.com, June 22, 2010 Tuesday 7:00 PM EST, , 11500 words, Briefing.com: Hourly In Play (R) - 19:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
14. Briefing.com, June 22, 2010 Tuesday 6:00 PM EST, , 11153 words, Briefing.com: Hourly In Play (R) - 18:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
15. Briefing.com, June 22, 2010 Tuesday 5:00 PM EST, , 10978 words, Briefing.com: Hourly In Play (R) - 17:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
16. Briefing.com, June 22, 2010 Tuesday 4:00 PM EST, , 9562 words, Briefing.com: Hourly In Play (R) - 16:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
17. Briefing.com, June 22, 2010 Tuesday 3:00 PM EST, , 8959 words, Briefing.com: Hourly In Play (R) - 15:00 ET
... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...
18. Briefing.com, June 22, 2010 Tuesday 2:00 PM EST, , 8503 words, Briefing.com: Hourly

In Play (R) - 14:00 ET

... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...

19. Briefing.com, June 22, 2010 Tuesday 1:00 PM EST, , 8387 words, Briefing.com: Hourly In Play (R) - 13:00 ET

... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...

20. Briefing.com, June 22, 2010 Tuesday 12:00 PM EST, , 7891 words, Briefing.com: Hourly In Play (R) - 12:00 ET

... all claims of VirnetX's U.S. Patent No. 6,502,135 and U.S. Patent No. **7,188,180** are patentable and valid. U.S. Patent No. 6,502,135, entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and U.S. Patent No. **7,188,180**, entitled "Method for Establishing Secure Communication Link Between Computers of Virtual ...

Source: **Combined Source Set 3**  - **News, Most Recent Two Years (English, Full Text)**

Terms: **7188180 or 7,188,180** (Suggest Terms for My Search)

View: Cite

Date/Time: Wednesday, December 14, 2011 - 6:29 PM EST

In

About LexisNexis | Privacy Policy | Terms & Conditions | Contact Us
Copyright © 2011 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the PETITION IN OPPOSITION TO PATENT OWNER'S PETITION TO VACATE *INTER PARTES* REEXAMINATION AND EXHIBITS A-M was served on:

MCDERMOTT WILL & EMERY
600 13TH STREET, NW
WASHINGTON DC 20005-3096

the attorneys of record for the assignee of USP 7,188,180 in accordance with MPEP § 2266.06 and 37 CFR §§ 1.248 and 1.903, on December 1, 2011.

In addition, it is noted that the Patent Owner has filed a Power of Attorney purportedly to change the attorney of record for this reexamination proceeding only (without changing the attorney of record for the underlying patent, in contravention of 37 U.S.C. § 1.33(c) and MPEP § 2622). Accordingly, a courtesy copy of the PETITION IN OPPOSITION TO PATENT OWNER'S PETITION TO VACATE *INTER PARTES* REEXAMINATION AND EXHIBITS A-M was served on:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

the attorneys identified in the Power of Attorney and who filed the Patent Owner Petition, on December 1, 2011.

/David L. McCombs/

David L. McCombs,
Registration No. 32,271

Exhibit H

U. Möller, "Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe," Diplomarbeit, Universität Hamburg (July 16, 1999), citing to *Martin* at page 77.

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

Universität Hamburg
Fachbereich Informatik

Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe

Diplomarbeit

Ulf Möller
<3umoelle@informatik.uni-hamburg.de>

16. Juli 1999

Betreuer: Prof. Dr. K. Brunnstein
Zweitbetreuer: Prof. Dr. M. Kudlek

Inhaltsverzeichnis

1	Einleitung	6
2	Grundlagen	8
2.1	WWW-Zugriffe	8
2.2	Personenbezogene Daten bei WWW-Zugriffen	9
2.2.1	Anbieter	9
2.2.1.1	IP-Adressen	9
2.2.1.2	Identifikations-Dienste	9
2.2.1.3	Vom Browser übertragene Daten	10
2.2.1.4	Server-Protokollierung	12
2.2.2	Netzbetreiber	12
2.3	Datenschutzanforderungen	12
2.4	Angreifermodelle	13
2.5	Definitionen	14
3	Protokolle zur Anonymisierung	15
3.1	Kryptographische Verfahren	15
3.1.1	Vertraulichkeit	15
3.1.1.1	Symmetrische Verschlüsselung	16
3.1.1.2	Asymmetrische Verschlüsselung	17
3.1.2	Integrität und Authentizität	19
3.2	Das ideale Modell der Anonymisierung	20
3.3	Das Mix-Netz	21
3.3.1	Anonymisierung von Nachrichten	21
3.3.2	Zuordbarkeit der Nachrichten	22
3.3.2.1	Umkodierung	22
3.3.2.2	Wiederholungen	22
3.3.2.3	Nachrichtenlänge	23
3.3.2.4	Umsortierung	24
3.3.3	Mix-Sequenzen	25
3.3.4	Aktive Angriffe	26
3.3.4.1	Verändern von Nachrichten	26
3.3.4.2	Deterministisches Padding im Mix-Netz	28
3.3.4.3	Isolieren von Nachrichten	29
3.3.4.4	Unterdrücken von Nachrichten	30
3.4	Mix-Netze in interaktiven Anwendungen	31

3.4.1	Verbindungsaufbau	32
3.4.2	Anonyme Verbindung	32
3.4.3	Schutz vor Verkehrsanalyse	33
3.4.4	Schutz gegen interne Angreifer	34
3.5	Anwendung für das WWW	35
3.6	Bestehende Systeme	35
3.6.1	Crowds	36
3.6.1.1	Verfahren	36
3.6.1.2	Sicherheit	36
3.6.2	JANUS	37
3.6.3	Freedom	37
3.6.3.1	Aufbau des Netzes	38
3.6.3.2	Client-Software	38
3.6.3.3	Anonyme Verbindungen	39
3.6.3.4	Sicherheit des Verfahrens	39
3.6.4	Onion Routing	40
3.6.4.1	Anonyme Verbindungen	40
3.6.4.2	Verbindung zwischen Onion-Routern	41
3.6.4.3	Sicherheit des Verfahrens	42
3.7	Entwurf eines Protokolls	43
4	Implementation	44
4.1	Wahl der Programmiersprache	44
4.2	HTTP-Proxy	45
4.2.1	Request-Nachrichten	46
4.2.2	Response-Nachrichten	47
4.2.3	Weitere Protokolle	48
4.2.4	Der filternde Client-Proxy AFproxy	48
4.3	WMix: Mix-Funktionalität	49
4.3.1	Konfiguration	49
4.3.2	Schlüsselverwaltung	49
4.3.3	Algorithmen	50
4.3.4	Verbindung zwischen zwei Mixen	51
4.3.5	Pakete	51
4.3.5.1	Padding	53
4.3.5.2	SessionKey	53
4.3.5.3	ReqChannel	53
4.3.5.4	Create	54
4.3.5.5	CreateAck	55
4.3.5.6	Error	55
4.3.5.7	Connect	55
4.3.5.8	ApplConnect	55
4.3.5.9	ApplClose, RApplClosed	55
4.3.5.10	Data	56
4.3.5.11	RData	56
4.3.5.12	Userdata, RUserdata	56
4.3.5.13	Close, Closed	57

4.3.6	Verbindung zum Anwender	57
4.3.6.1	NODE	57
4.3.6.2	CONNECT	58
4.3.6.3	DATA	58
4.3.6.4	CLOSE	59
4.3.6.5	QUIT	59
4.4	Aufbau der Mix-Implementation WMix	60
4.5	Die Verschlüsselungsbibliothek OpenSSL	61
4.5.1	OAEP	61
4.5.2	Der Zufallszahlengenerator	61
5	Performanz	63
5.1	Auswirkungen für den Anwender	63
5.1.1	Verzögerung	63
5.1.2	Durchsatz	64
5.2	Praktische Erprobung	64
5.2.1	Durchführung	64
5.2.2	Auswertung	65
5.2.3	Ergebnis	66
6	Sicherheit	67
6.1	Verkehrsanalyse	67
6.1.1	Externer Angreifer	67
6.1.2	Interner Angreifer	68
6.2	Zeitverhalten	68
6.2.1	Kryptographische Operationen	69
6.2.2	Verzögerung durch andere Prozesse	69
6.3	Nicht-anonyme Datenübertragung	69
6.4	Aktive Angriffe	70
6.4.1	Externer Angreifer	70
6.4.2	Interner Angreifer	70
7	Zusammenfassung und Ausblick	72
7.1	Mögliche Weiterentwicklungen	72
7.1.1	Verbesserung der Benutzerschnittstelle	73
7.1.2	Anpassungen des Mix-Protokolls	73
7.2	Vorschlag einer praktischen Mix-Architektur	73
	Literaturverzeichnis	75
	Index	80

Abbildungsverzeichnis

2.1	Beispiel für einen HTTP-Request	11
3.1	Anwendung einer Mix-Sequenz	22
3.2	Schutz der Kommunikationsbeziehung durch Mix-Kaskaden	24
3.3	Anonyme Verbindung	41
4.1	WWW-Zugriffe: direkt und über einen Proxy	46
4.2	Create-Paket in einem Data-Paket	53
4.3	Abfolge der Kommandos	58
4.4	Dialog zwischen Proxy und lokalem Mix	59
5.1	Dauer einer Mix-Runde in 1/1000 Sekunden	65
6.1	Mögliche Angriffe gegen das Mix-Netz	67

Abkürzungsverzeichnis

ACI	Anonymous Connection Identifier
DES	Data Encryption Standard
ftp	File Transfer Protocol
HMAC	Hash-based MAC
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IV	Initial Value
MAC	Message Authentication Code
MDC	Modification Detection Code
OAEP	Optimal Asymmetric Encryption Padding
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standard
PRNG	Pseudo-Random Number Generator
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WWW	World Wide Web

Kapitel 1

Einleitung

Seit 1993 hat sich das WWW zu einem der wichtigsten Internet-Dienste entwickelt. Mit eigenen Angeboten sind im World Wide Web mittlerweile nahezu alle Zeitungen und Zeitschriften vertreten; eine zunehmende Anzahl kommerzieller Datenbanken ist über das WWW zu erreichen. Hinzu kommen neue Multimedia-Dienste und ungezählte private Angebote.

Bei traditionellen Medien ist dem Verlag nur bekannt, wer die Abonnenten einer Publikation sind; über deren Lesegewohnheiten liegen keine Daten vor. Es ist möglich, Zeitschriften am Kiosk zu erwerben, ohne daß eine Datenspur entsteht. Auch über die Zuhörer bzw. Zuschauer von Radio- und Fernsehprogrammen fallen normalerweise keine personenbezogenen Daten an.

Im Internet ist dies anders. Wenn der WWW-Browser des Nutzers eine Verbindung zum Server des Anbieters aufbaut, um Informationen abzurufen, fallen dort personenbezogene Daten an, die von vielen WWW-Servern in Dateien protokolliert werden. Internet-Provider können die Daten über sämtliche Netz-Zugriffe ihrer Kunden speichern und auswerten und so umfangreiche Persönlichkeitsprofile gewinnen.

Das Interesse der Anbieter an Daten über ihre Nutzer wird schon an dem großen Aufwand deutlich, der für die Ermittlung von Einschaltquoten von Fernsehsendern und für Leserbefragungen von Zeitschriften getrieben wird. Wenn Betreiber von WWW-Servern personenbezogene Daten ohne Einwilligung oder sogar ohne das Wissen der Nutzer sammeln und auswerten, wird deren Recht auf informationelle Selbstbestimmung verletzt. Die Rechte der Nutzer sind in Datenschutzgesetzen festgeschrieben; der Nutzer hat aber keine Möglichkeit zu überprüfen, ob der Anbieter diese Regelungen tatsächlich einhält. Bei der Vielzahl der Anbieter ist auch keine umfassende Kontrolle durch Datenschutzbehörden möglich. Zudem befinden sich viele Server in Staaten wie den USA, in denen die Auswertung personenbezogener Daten im allgemeinen zulässig ist.

Zuverlässig läßt sich der Mißbrauch personenbezogener Daten im Internet daher nur mit technischen Mitteln verhindern. Erfolgt der Zugriff

des Nutzers auf WWW-Server anonym, fallen dort gar keine personenbezogenen Daten an. Anonymisierungsverfahren für WWW-Zugriffe sind daher ein wirkungsvolles Verfahren, um den Datenschutz in diesem neuen Medium durchzusetzen.

David Chaum hat 1981 mit dem Mix-Netz das erste kryptographische Anonymisierungsverfahren für E-Mail entwickelt. In der Folgezeit wurden Verfahren vorgeschlagen, die anonyme Zugriffe auf das WWW ermöglichen. Der derzeit meistgenutzte Anonymisierungsdienst ist ein von der Firma *The Anonymizer Inc.* betriebener Server. Eine größere Sicherheit bieten auf dem Mix-Netz beruhende Verfahren wie *Onion-Routing* und *Freedom*. Die Implementation eines derartigen Anonymisierungsverfahrens ist Gegenstand dieser Arbeit.

Kapitel 2

Grundlagen

2.1 WWW-Zugriffe

Bei Zugriffen auf das WWW ruft der Nutzer mit Hilfe eines als *Browser* bezeichneten Programms Daten von *Servern* verschiedener Anbieter ab. Als Adresse eines WWW-Dokuments dient ein eindeutiger Bezeichner, üblicherweise ein *Uniform Resource Locator (URL)*, der das Übertragungsprotokoll, eine Internet-Adresse sowie einen Pfadnamen für das Dokument angibt.

WWW-Browser beherrschen eine Vielzahl von Übertragungsprotokollen und Dateiformaten bzw. Datentypen. Für die Übertragung von WWW-Seiten wird üblicherweise das *Hypertext Transfer Protocol (HTTP)* [Fielding 1997] auf einer TCP/IP-Verbindung verwendet. Der Browser baut eine Verbindung zum HTTP-Port des Servers auf und sendet eine Anfrage (*Request*) mit dem URL der gewünschten WWW-Seite. Der Server antwortet mit einer Nachricht, die das gewünschte Dokument enthält (*Response*). HTTP-Nachrichten bestehen aus einem *Message Header*, der Fehlermeldungen und Angaben zum Datentyp des übertragenen Dokuments enthalten kann, sowie einem *Message Body*, der das zu übertragende Dokument enthält. Dokumente in der Beschreibungssprache HTML [Berners-Lee 1995] enthalten neben dem eigentlichen Text Informationen darüber, wie der Text darzustellen ist, und Verknüpfungen zu weiteren Daten, die zum Teil vom Benutzer ausgewählt werden können, zum Teil aber auch – wie beispielsweise in einem HTML-Dokument enthaltene Grafiken – vom Browser automatisch abgerufen und dargestellt werden.

Statt direkte HTTP-Zugriffe zum jeweiligen Server durchzuführen, werden *Proxies* eingesetzt, wenn eine direkte Verbindung nicht möglich oder nachteilig ist. Der Browser sendet die Anfragen dabei an den vorinstallierten Proxy, dieser leitet sie an den WWW-Server weiter. Proxy-Caches speichern oft abgerufene Seiten lokal, um schnellere Antwortzeiten zu erreichen und das Übertragungsvolumen zu reduzieren. Proxies werden auch eingesetzt, um Clients bei der Verwendung eines Firewall

den Zugriff auf externe Daten zu ermöglichen, ohne ihnen direkte HTTP-Verbindungen zu externen Servern erlauben zu müssen.

2.2 Personenbezogene Daten bei WWW-Zugriffen

Bei WWW-Zugriffen entsteht eine Vielzahl von Daten, die Rückschlüsse über Interessen und Verhaltensweisen des Nutzers geben. Zu unterscheiden ist dabei, welche Daten ein Informationsanbieter und welche ein Netzbetreiber erhält.

2.2.1 Anbieter

Der Betreiber eines WWW-Servers erhält verschiedene Daten über die Personen, die sein Angebot nutzen. Diese Daten werden ohne Kontrollmöglichkeit und oft sogar ohne Wissen der Nutzer übermittelt.

2.2.1.1 IP-Adressen

Wird zwischen dem Browser des Nutzers und dem WWW-Server eine HTTP-Verbindung aufgebaut, erfährt der Anbieter notwendigerweise, von welcher IP-Adresse der Abruf durchgeführt wird. Arbeitsplatzrechner mit permanenter Internetverbindung haben in der Regel eine fest zugeordnete IP-Nummer, so daß der Nutzer eines Ein-Personen-Systems durch diese Angabe eindeutig identifiziert ist.

Bei der Modem-Einwahl, wie Privatkunden sie üblicherweise nutzen, wird die IP-Nummer dagegen in der Regel dynamisch vergeben. Aus der Adresse läßt sich dann nur entnehmen, über welchen Internet-Provider der Zugriff durchgeführt wurde.

Auch wenn ein Proxy verwendet wird, ist der Nutzer nicht an der IP-Nummer zu erkennen.¹ Da die Verbindung zum Server durch den Proxy hergestellt wird, ist aus der IP-Nummer nur zu erkennen, daß der Zugriff von einem Angehörigen derjenigen Organisation bzw. einem Kunden desjenigen Providers erfolgt ist, der den Proxy betreibt. Welche Auswirkungen dies hat, hängt von der Anzahl der Benutzer ab. Bei einer kleinen Zahl von Nutzern ist damit zu rechnen, daß nur einer von ihnen auf einen bestimmten Server zugreift, so daß die Adreß-Angabe auch in diesem Fall auf die Person zurückschließen läßt.

2.2.1.2 Identifikations-Dienste

Einige frühe HTTP-Implementationen sendeten bei Zugriffen auf WWW-Server eine From-Zeile mit der E-Mail-Adresse des Nutzers, ähnlich wie

¹Manche Proxies fügen allerdings eine Header-Zeile X-Forwarded-For: ein, aus der die IP-Nummer des Nutzers hervorgeht.

es bei dem älteren ftp-Protokoll üblich ist, die E-Mail-Adresse als Paßwort anzugeben. In [Fielding 1997] ist die Übertragung dieser Header-Zeile aus Datenschutzgründen allerdings nur nach ausdrücklicher Bestätigung des Nutzers vorgesehen.

Es gibt jedoch weitere Internet-Dienste, die der Identifikation von Nutzern dienen. Über den *finger*-Dienst [Zimmerman 1991] lassen sich Namen, E-Mail-Adressen und weitere Informationen über die auf einem Computer eingeloggten Personen feststellen. Sofern der Betreiber des Systems diesen Dienst aktiviert hat, läßt sich so der Bezug zwischen einer IP-Nummer und einer Person herstellen. Nur wenn der Zugriff über einen Proxy erfolgt ist, führt eine *finger*-Anfrage nicht zu der gewünschten Information. Dann ist es jedoch möglich, Anfragen an alle Systeme in dem jeweiligen Subnetz zu richten, in dem sich der Proxy befindet. In vielen Fällen ist unter den Personen, deren Namen so festgestellt werden, auch der tatsächliche Nutzer. Wenn zu verschiedenen Zeiten Zugriffe erfolgen, läßt sich schließen, daß der fragliche Nutzer derjenige sein muß, der während aller Zugriffe eingeloggt war.

Das für Audit-Zwecke gedachte Identifikations-Protokoll [Johns 1993] übermittelt eine den Eigentümer einer bestimmten TCP-Verbindung identifizierende Zeichenkette. Wenn der *ident*-Dienst auf dem System des Nutzers installiert ist, kann ein Server-Betreiber so feststellen, wer einen Zugriff durchgeführt hat. Nur in wenigen Fällen ist die Kooperation des Systembetreibers erforderlich, um aus der *ident*-Zeichenkette auf die Identität des Nutzers zu schließen; üblicherweise wird der Login-Name des Nutzers übermittelt. Bei T-Online, dem größten Internet-Zugangsanbieter Deutschlands, ist dies in der Regel die Telefonnummer des Kunden. Auf Antrag teilt T-Online auch eine andere Nummer zu; da diese jedoch auch in allen E-Mail-Nachrichten und Usenet-Artikeln des Nutzers übertragen wird, ist es häufig möglich, dessen Namen beispielsweise über eine Suchmaschine festzustellen [Möller 1998].

2.2.1.3 Vom Browser übertragene Daten

Die verbreitetsten Browser *Internet Explorer* und *Netscape Navigator* übertragen als Bestandteil einer HTTP-Anfrage neben dem URL eine Reihe weiterer Daten. Übermittelt werden beispielsweise Angaben zur verwendeten Browser- und Betriebssystemversion und der Bildschirmauflösung, eine Liste akzeptierter Datentypen und Angaben über die Sprache des Nutzers. Diese Informationen können dazu dienen, den Nutzer zu identifizieren. Da Proxies diese Angaben im Normalfall weiterleiten, ist die Identifikation des Nutzers auch möglich, wenn er einen Proxy verwendet.

Wenn der Nutzer einem Hypertext-Link folgt, übertragen Browser zudem einen *Referer*-Header, der den URL der Seite enthält, von der der Nutzer gekommen ist. Damit läßt sich verfolgen, wie er sich durch das

```
GET / HTTP/1.0
If-Modified-Since: Tuesday, 20-Oct-98 15:07:06 GMT; length=7000
Connection: Keep-Alive
User-Agent: Mozilla/4.07 [en] (X11; I; SunOS 5.6 sun4u)
Host: echo.znet.de:8888
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
        image/png, */*
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

Abbildung 2.1: Beispiel für einen HTTP-Request

WWW-Angebot bewegt, mit welcher Such-Anfrage er auf einen Server gelangt ist oder welchen Namen eine private Datei hat, von der aus er den Server aufruft.

WWW-Browser übertragen auf Anforderung des Servers hin während einer Sitzung oder auch über mehrere Sitzungen hinweg in den HTTP-Anfragen Zustandsinformationen, die als *Cookies* bezeichnet werden [Kristol 1997]. Dadurch können beispielsweise personalisierte Einstiegsseiten implementiert werden. Häufig werden Cookies allerdings im Zusammenhang mit Werbeeinblendungen verwendet. Deren Betreiber erfährt im Referer-Header, welche Seite abgerufen wurde, und kann die Anfrage durch einen Cookie einem einzelnen Nutzer zuordnen. Da viele Suchmaschinen und Inhalteanbieter an solche Werbeanbieter angeschlossen sind, entstehen dort umfassende Nutzerprofile, in denen unter Umständen sämtliche Suchanfragen des Nutzers enthalten sind.

Netscape 4 bietet die Möglichkeit, zu WWW-Seiten themenverwandte Seiten anderer Anbieter zu finden. Dazu sendet der Browser einen HTTP-Request mit dem URL der jeweils abgerufenen Seite an einen Netscape-eigenen Server. In der Default-Einstellung wird diese Anfrage während des Ladens jeder WWW-Seite automatisch durchgeführt, nachdem der Nutzer den „What's related“-Button einmal benutzt hat. Die Firma Netscape erhält dadurch eine vollständige Liste aller von dem Nutzer gelesenen Seiten.

Weitere Möglichkeiten zur Übertragung persönlicher Daten des Nutzers ergeben sich daraus, daß WWW-Browser aus dem Netz geladene Programme ausführen können. ActiveX-Controls haben alle Zugriffsrechte des Nutzers auf System-Ressourcen. Bei anderen Konzepten, wie zum Beispiel Java-Applets und JavaScript, sind Zugriffsbeschränkungen vorgesehen; es wurden jedoch verschiedene Fehler bekannt, durch die nicht vorgesehene Zugriffe auf Daten des Nutzers möglich sind. Beispielsweise ist es in vielen Browser-Versionen möglich, mit JavaScript-Programmen ohne Wissen des Nutzers eine E-Mail-Nachricht in dessen Namen zu verschicken.

2.2.1.4 Server-Protokollierung

Der derzeit meistverwendete WWW-Server Apache protokolliert bei jedem Zugriff standardmäßig das aufgerufene Objekt, die Internet-Adresse des Abrufers sowie Datum und Uhrzeit. Auch die Protokollierung von Referer-Zeilen ist weit verbreitet.

2.2.2 Netzbetreiber

Der Netzbetreiber, über den der Nutzer Zugang zum Internet erhält, kann die gesamte Kommunikation des Nutzers beobachten. Für Proxies sind umfangreiche Protokolldateien nicht ungewöhnlich. Der Proxy *Squid* speichert in der Datei `access.log` beispielsweise zu jedem Zugriff den Zeitpunkt, die Adresse des Clients sowie auf Wunsch das Ergebnis einer `ident`-Abfrage, den abgerufenen URL, und die Größe der übertragenen Datei [Wierda 1997].

Auch wenn der Nutzer keinen Proxy nutzt, kann der Netzbetreiber auf der TCP-Ebene auf die Kommunikation zugreifen. Nur wenn die Übertragung verschlüsselt erfolgt (beispielsweise mittels SSL [Freier 1996]), hat er keinen Zugriff auf die Inhaltsdaten. Die Adressen der Kommunikationspartner und die Länge der übertragenen Daten liegen allerdings auch dann vor und können zur Identifikation der abgerufenen Dateien verwendet werden.

Eine Verbindung zu einem WWW-Server führt üblicherweise durch die Netze vieler private Betreiber; welche Betreiber in welchen Ländern beteiligt sind, ist dem Nutzer zumeist nicht bekannt. Die Übertragung kann an jedem beteiligten Netzknoten abgehört und automatisch nach interessanten Daten durchsucht werden.

2.3 Datenschutzerfordernungen

Eine Anonymisierung des Zugriffs auf WWW-Server kann wirksamen Datenschutz für den Nutzer gewährleisten. Zumeist benötigt der Anbieter keine Informationen über seine individuellen Kunden: Statistiken über die Nutzung seines Angebots und sogar die Bezahlung kostenpflichtiger Dienste sind auch dann möglich, wenn der Zugriff anonym erfolgt. Es ist somit möglich, eine datenschutzfreundliche Infrastruktur aufzubauen, die auch die Interessen der Anbieter berücksichtigt. Ziel dieser Infrastruktur ist demzufolge, daß der Nutzer gegenüber dem Betreiber *anonym* bleibt.

Um zu verhindern, daß der Betreiber Wissen über eine Person ansammeln kann, das deren Anonymität gefährden würde, sollten verschiedene Zugriffe eines Nutzers auf den Server in der Regel *unverkettbar* sein. In bestimmten Fällen ist es jedoch wünschenswert, personalisierte Zugriffe zu

ermöglichen, ohne daß der Betreiber dabei die Identität des Nutzers kennen sollte (*Pseudonymität*). Die Pseudonyme eines Nutzers für verschiedene Rollen sollten dann unverkettbar sein.

Zudem sollten Zugriffe auf WWW-Server für Unbeteiligte *unbeobachtbar* erfolgen. Dies ist auch dann wünschenswert, wenn der Nutzer sich dem Betreiber des Servers gegenüber identifiziert. Unbeobachtbarkeit beinhaltet nicht nur die Vertraulichkeit der *Inhaltsdaten*, sondern auch die der Information, wer wann von wem Daten abrufen (*Verkehrsdaten*).

Ein datenschutzkonformes Kommunikationssystem soll somit die Anforderungen nach Anonymität, Unverkettbarkeit, Pseudonymität und Unbeobachtbarkeit erfüllen [Pfitzmann 1990, Rannenberg 1995].

2.4 Angreifermodelle

Um die Sicherheit eines Verfahrens zu bewerten, werden verschiedene Angreifermodelle betrachtet. Ein **Angreifer** ist jemand oder etwas – zum Beispiel eine Person oder ein Computer –, der versucht, nicht für ihn bestimmte Informationen zu erhalten, falsche Nachrichten zu senden oder die Erbringung eines Dienstes zu verhindern. Angreifer kann sowohl ein Außenstehender als auch ein Nutzer oder Betreiber eines Netzdienstes sein.

Ein **passiver** Angreifer kann einen Teil oder sämtliche Kommunikationsverbindungen abhören. Ein **aktiver** Angreifer kann darüberhinaus übertragene Nachrichten verfälschen, verzögern und unterdrücken und eigene Nachrichten übertragen, indem er versucht, als legitimer Sender zu erscheinen.

Ein Angreifer, der nur Zugriff auf die Kommunikationsverbindungen hat, heißt **externer** Angreifer. Sind legitime Kommunikationsteilnehmer, also Nutzer oder Betreiber eines Dienstes, an einem Angriff beteiligt, spricht man von einem **internen** Angreifer.

Häufig ist es möglich, durch die Auswertung der übertragenen Datenmengen und der Sende- und Empfangszeitpunkte Informationen über kryptographisch gesicherte Kommunikation zu gewinnen. Solche Angriffe werden als **Verkehrsanalyse** (*traffic analysis*) bezeichnet.

Wenn der Angreifer sämtliche Kommunikationsverbindungen abhören kann, heißt er **omnipräsenter** Angreifer. Häufig ist die Annahme sinnvoll, daß bestimmte Verbindungen dem Angreifer nicht zugänglich sind. Auch bei omnipräsenten Angreifern ist vorausgesetzt, daß ein Teil der geheimen Schlüssel dem Angreifer nicht bekannt ist; andernfalls wäre kein Schutz durch kryptographische Verfahren möglich.

Weiter werden Angreifer danach unterschieden, welche Berechnungen sie durchführen können, um beispielsweise eine Verschlüsselung zu brechen.

2.5 Definitionen

R_I bezeichne, daß der Nutzer I eine Rolle R wahrnimmt, beispielsweise Sender oder Empfänger einer Nachricht ist. $P(A)$ ist die Wahrscheinlichkeit eines Ereignisses A , $P(A|B)$ die bedingte Wahrscheinlichkeit für A unter der Bedingung, daß das Ereignis B eingetreten ist.

Ein Nutzer A ist in der Rolle R **anonym** bezüglich eines Angreifers E und einer Menge \mathcal{A} von nicht mit E kooperierenden Nutzern (*Anonymitätsmenge*), wenn E nicht feststellen kann, daß A die Rolle R wahrgenommen hat.

A heißt **perfekt anonym** in der Rolle R bezüglich E und \mathcal{A} , wenn nach jeder für E möglichen Beobachtung B gilt: $\forall I \in \mathcal{A}: P(R_I) = P(R_I|B)$, d. h. keine Beobachtung B liefert E zusätzliche Informationen darüber, wer die Rolle R wahrnimmt [Pfitzmann 1990].

Je nach der dabei betrachteten Rolle spricht man von *Sender-Anonymität* und *Empfänger-Anonymität*. Um einen WWW-Zugriff durchzuführen, muß eine Anfrage gesendet und die Antwort des Servers empfangen werden; damit der Zugriff anonym bleibt, sind also Sender- und Empfänger-Anonymität notwendig.

Ein Ereignis X heißt für einen Angreifer E **unbeobachtbar**, wenn für jede für E mögliche Beobachtung B gilt: $P(X) = P(X|B)$, d. h. daß die Beobachtung E keine zusätzlichen Informationen über X liefert.

Kapitel 3

Protokolle zur Anonymisierung

Kryptographische Verfahren dienen dem Schutz der Vertraulichkeit und Authentizität von Daten. Durch Protokolle, in denen kryptographische Operationen verwendet werden, kann die anonyme Übertragung von Nachrichten realisiert werden.

3.1 Kryptographische Verfahren

3.1.1 Vertraulichkeit

Zum Schutz vor unbefugter Kenntnisnahme können Daten verschlüsselt werden. Ein Kryptosystem besteht aus einem Klartextrraum \mathcal{M} , einem Geheimtextraum \mathcal{C} , einem Schlüsselraum \mathcal{K} , einer Menge $\{E_e: e \in \mathcal{K}\}$ von Verschlüsselungsfunktionen $E_e: \mathcal{M} \rightarrow \mathcal{C}$ (bei *probabilistischen* Kryptosystemen ist E_e statt dessen ein nichtdeterministischer Algorithmus) und einer korrespondierenden Menge $\{D_d: d \in \mathcal{K}\}$ von Entschlüsselungsfunktionen $D_d: \mathcal{C} \rightarrow \mathcal{M}$ mit der Eigenschaft, daß es zu jedem $e \in \mathcal{K}$ einen Schlüssel d gibt, so daß $D_d(E_e(m)) = m$ für alle $m \in \mathcal{M}$ [Menezes 1997]. $\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e\}$ und $\{D_d\}$ müssen nicht geheimgehalten werden.

Ein Verschlüsselungsverfahren ist **sicher**, wenn es einem auf effiziente Berechnungen beschränkten Angreifer nicht möglich ist, ohne Kenntnis des Schlüssels d aus einem Geheimtext systematisch Informationen über den entsprechenden Klartext – über die Tatsache hinaus, daß eine Nachricht der gegebenen Länge vorliegt – zurückzugewinnen.

Informationstheoretisch oder **perfekt sicher** ist ein Verschlüsselungsverfahren, wenn ein Angreifer mit unbegrenzter Rechenkapazität von der Länge abgesehen keine Informationen über den Klartext erhalten kann. Perfekte Sicherheit ist nur möglich, wenn der Schlüssel mindestens so lang ist wie die (eventuell vorher komprimierte) zu übertragende Nachricht. Durch das daraus resultierende Schlüsselverteilungsproblem sind

perfekt sichere Verfahren für die Anwendung in offenen Netzen unpraktikabel. Die Bewertung von in der Praxis eingesetzten Verfahren als sicher beruht auf der Annahme, daß für bestimmte Probleme keine effizienten Algorithmen existieren und daß bestimmte Berechnungen in der einem Angreifer zur Verfügung stehenden Zeit nicht praktikabel sind. Wenn gezeigt werden kann, daß das Brechen eines Systems so schwer ist, wie die Lösung eines wohlbekannten und als schwierig angesehenen Problems zu finden, wird es auch als **kryptographisch sicher** bezeichnet.

Angriffe auf Verschlüsselungsverfahren werden danach unterschieden, ob der Angreifer nur Geheimtexte beobachtet (*ciphertext-only attack*), Paare von Klartexten und zugehörigen Geheimtexten kennt (*known-plaintext attack*), Klartexte selbst auswählen kann und die zugehörigen Geheimtexte erhält (*chosen-plaintext attack*) oder Geheimtexte auswählen kann und die entsprechenden Klartexte erhält (*chosen-ciphertext attack*).

3.1.1.1 Symmetrische Verschlüsselung

In einem **symmetrischen** Verschlüsselungsverfahren kann d einfach aus e bestimmt werden, üblicherweise ist $e = d$. Dieser **geheime Schlüssel** muß vorab über einen sicheren Kanal ausgetauscht werden.

Ein symmetrisches Verschlüsselungsverfahren, durch das ein n -Bit-Klartext auf einen n -Bit-Geheimtext abgebildet wird, heißt **Blockchiffre** mit Blocklänge n . Um Klartexte beliebiger Länge zu verschlüsseln, können Blockchiffren in verschiedenen **Betriebsmodi** eingesetzt werden [Menezes 1997]. Im *ECB-Modus (Electronic Code Book)* wird der Klartext in Blöcke der Größe n unterteilt und alle Blöcke unabhängig voneinander verschlüsselt. Identische Klartextblöcke ergeben daher identische Geheimtextblöcke, so daß Datenmuster im Geheimtext erkennbar bleiben und Angreifer Blöcke unbemerkt vertauschen oder einfügen können. Für Nachrichten, die länger als n Bits sind, ist dieser Modus somit unsicher. Im *CBC-Modus (Cipher Block Chaining)* wird ein Initialisierungswert (*initial value, IV*) verwendet, von dem der erste Geheimtextblock neben dem Schlüssel und dem ersten Klartextblock zusätzlich abhängt; alle folgenden Geheimtextblöcke hängen vom jeweils vorhergehenden Geheimtextblock, dem Schlüssel und dem jeweiligen Klartextblock ab. Damit ergeben sich für die Verschlüsselung eines Klartextes mit demselben Schlüssel genau dann identische Geheimtexte, wenn auch der IV identisch ist. Der IV muß im Gegensatz zum Schlüssel nicht geheimgehalten werden.

Das bekannteste symmetrische Verschlüsselungsverfahren ist der **Data Encryption Standard (DES)** [FIPS 1980]. DES ist eine Blockchiffre mit 56-Bit-Schlüsseln. Aufgrund des kleinen Schlüsselraums ist es mit begrenzten Ressourcen möglich, den Klartext zurückzugewinnen, indem der Geheimtext systematisch mit allen denkbaren Schlüsseln entschlüsselt wird; DES ist daher unsicher [EFF 1998]. Durch die Verwendung von **Triple-DES** [Menezes 1997] kann dieser Angriff verhindert werden. Praktikable Angriffe auf Triple-DES sind nicht bekannt; dieser Algorithmus

wird daher allgemein als sicher angesehen. Ein *Advanced Encryption Standard (AES)* wird derzeit entwickelt.

3.1.1.2 Asymmetrische Verschlüsselung

Ein Kryptosystem, das auch dann sicher ist, wenn der Angreifer E_e kennt, heißt **asymmetrisch** (*Public-Key-Verschlüsselung*). e kann in dem Fall veröffentlicht werden und heißt daher auch **öffentlicher Schlüssel**; d ist der **private Schlüssel**.

Asymmetrische Kryptosysteme beruhen auf *Einwegfunktionen mit Falltür*. Eine **Einwegfunktion** ist eine effizient berechenbare Funktion, deren Umkehrung sich nur mit vernachlässigbarer Wahrscheinlichkeit effizient berechnen läßt; bei einer Einwegfunktion mit Falltür ist die Umkehrung nur mit Kenntnis eines geheimen Parameters (*Falltürinformation*) effizient zu berechnen. Ob es derartige Funktionen wirklich gibt, ist nicht bekannt. Funktionen, von denen angenommen wird, daß sie diese Eigenschaft erfüllen, beruhen beispielsweise auf der Schwierigkeit, Zahlen in ihre Primfaktoren zu zerlegen oder diskrete Logarithmen zu berechnen.

Damit ein asymmetrischer Verschlüsselungsalgorithmus sicher ist, muß er einen von verschiedenen möglichen Geheimtexten zufällig auswählen (*probabilistische Verschlüsselung*), wobei die Menge der möglichen Geheimtexte so groß ist, daß die Zuordnung eines Geheimtextes zu einem gegebenen Klartext nicht durch systematisches Ausprobieren aller Verschlüsselungen dieses Klartextes festgestellt werden kann. Bei *deterministischen* asymmetrischen Kryptosystemen ist die Entschlüsselung von Nachrichten aus einem kleinen, bekannten Klartextraum trivial [Goldreich 1997, Bellare 1997].

Ein Kryptosystem heißt *plaintext aware*, wenn es ohne Kenntnis des Klartextes nicht praktikabel ist, einen gültigen Geheimtext zu erzeugen. Bei Kryptosystemen ohne *plaintext awareness* besteht die Möglichkeit, daß ein Angreifer einen Geheimtext durch adaptive *chosen ciphertext*-Angriffe entschlüsseln kann. Bei *chosen ciphertext*-Angriffen erzeugt der Angreifer Geheimtexte, deren Klartext in einer vorhersagbaren Weise vom gesuchten Klartext abhängt, und veranlaßt den Schlüsselinhaber dazu, ihm Informationen über den Klartext mitzuteilen. Da die Entschlüsselung in vielen Anwendungen automatisch erfolgt, sind derartige Angriffe oft praktikabel. Dies ist zum Beispiel bei RSA-Verschlüsselung nach PKCS #1 Version 1.5 der Fall [Bleichenbacher 1998].

Das verbreitetste asymmetrische Kryptosystem ist **RSA** [Kaliski 1998]. Ein öffentlicher RSA-Schlüssel besteht aus zwei natürlichen Zahlen (n, e) , wobei n das Produkt zweier verschiedener Primzahlen p und q ist und $\text{ggT}(e, (p-1)(q-1)) = 1$ gilt. Zu diesem Schlüssel gehört ein geheimer Schlüssel d mit $ed \equiv 1 \pmod{(p-1)(q-1)}$. d kann bei Kenntnis von p und q effizient berechnet werden.

Um eine Nachricht zu verschlüsseln, wird anhand einer *Kodierungsvorschrift* eine den Klartext repräsentierende natürliche Zahl m gebildet und der Geheimtext durch die Verschlüsselungsprimitive $c := m^e \bmod n$ berechnet. Mit dem geheimen Schlüssel kann $m = c^d \bmod n$ berechnet werden. Durch eine Dekodierungsvorschrift wird daraus der Klartext gewonnen oder aber ein Entschlüsselungsfehler festgestellt.

Wenn es möglich ist, große Zahlen zu faktorisieren, es also einen effizienten Algorithmus gibt, um p und q aus dem öffentlichen Modulus n zu errechnen, ist RSA unsicher. Der beste hierfür bekannte Algorithmus ist das *General Number Field Sieve (GNFS)*. Die Faktorisierung eines 1024 Bit großen RSA-Modulus würde damit $3 \cdot 10^{11}$ MIPS-Jahre benötigen, so daß RSA bei dieser Schlüssellänge als sicher angesehen wird [Wiener 1998].

Wenn RSA mit geeigneten Kodierungsvorschriften verwendet wird und bei der Schlüsselerzeugung bestimmte Randbedingungen [Menezes 1997] beachtet werden, ist kein effizienterer Angriff als die Faktorisierung von n bekannt. Um ein sicheres Kryptosystem zu erhalten, muß die Kodierungsvorschrift probabilistisch sein. Die Dekodierungsvorschrift muß zur Verhinderung von *chosen plaintext*-Angriffen sicherstellen, daß ein gültiger Geheimtext nicht erzeugt werden kann, ohne den dazugehörigen Klartext zu kennen.

OAEP (*Optimal Asymmetric Encryption Padding*) [Bellare 1995, Kaliski 1998] ist eine probabilistische Kodierungsvorschrift, für die Sicherheit von RSA unter der Annahme bewiesen werden kann, daß die verwendete Hashfunktionen ideal ist (*random oracle*-Modell) und daß die Verschlüsselungsprimitive eine Einwegfunktion ist.

Das **EIGamal**-Kryptosystem beruht dagegen auf der Schwierigkeit, diskrete Logarithmen zu berechnen. Auch hierfür werden Schlüssellängen ab 1024 Bit als sicher angesehen; für auf elliptischen Kurven basierende Verfahren gelten Schlüssellängen ab 160 Bit als sicher [Wiener 1998].

Der Aufwand für asymmetrische Ver- und Entschlüsselung ist i. a. höher als der für symmetrische. Asymmetrische Verfahren werden in der Praxis mit symmetrischen zu *Hybridverfahren* kombiniert, indem nur ein zufällig gewählter Sitzungsschlüssel für das symmetrische Verfahren asymmetrisch verschlüsselt wird.

Eine Anforderung, die man an Kryptosysteme zusätzlich stellen kann, besteht darin, daß ein Angreifer im Nachhinein selbst dann keine Informationen über in der Vergangenheit übertragene Nachrichten gewinnen darf, wenn einer der dauerhaften privaten Schlüssel zu einem späteren Zeitpunkt kompromittiert wird. Diese als **forward secrecy** bezeichnete Eigenschaft kann durch ein Protokoll zum Vereinbaren geheimer Sitzungsschlüssel, beispielsweise durch den Diffie-Hellman-Algorithmus, erreicht werden [Goldwasser 1997]. Sie läßt sich auch bei RSA erzielen, indem Schlüssel nur eine kurze Gültigkeitsdauer erhalten und die geheimen Schlüssel nach deren Ablauf gelöscht werden.

3.1.2 Integrität und Authentizität

Unter *Integrität* versteht man, daß Informationen vor unbefugter Veränderung geschützt sind; *Authentizität* ist die Gewährleistung, daß Daten tatsächlich vom angegebenen Absender stammen.

Zum Erreichen dieser Ziele werden **kryptographische Hashfunktionen** eingesetzt. Eine *Hashfunktion* ist eine effizient berechenbare Funktion, die Zeichenketten beliebiger Länge auf Zeichenketten einer festen Länge („Hash-Werte“) abbildet. Eine Hashfunktion h heißt *sicher* oder *kryptographische Hashfunktion*, wenn es nicht praktikabel ist, zwei Eingaben x und y zu finden, so daß $h(x) = h(y)$ gilt (*Kollisionsresistenz*), oder zu einem gegebenen Hash-Wert y ein x mit $h(x) = y$ zu finden. Verbreitete Hash-Algorithmen sind MD5, in dem jedoch Schwächen gefunden wurden, und SHA-1 [FIPS 1995]. Die Hash-Werte von SHA-1 sind 160 Bit groß.

Hash-Werte können als **Modification Detection Codes (MDC)** die Integrität verschlüsselter Daten sicherstellen. Hierfür berechnet der Sender einer Nachricht x den Hash-Wert $h(x)$ und überträgt $x || h(x)$ verschlüsselt. Hierbei bezeichne $||$ die Konkatenation von Bitketten. Der Empfänger entschlüsselt die empfangene Nachricht und berechnet ebenfalls $h(x)$. Wenn die Werte übereinstimmen, ist die Nachricht nicht verfälscht worden.

Zur Sicherung der Authentizität von Daten können **Message Authentication Codes (MAC)** eingesetzt werden. Der Sender einer Nachricht x berechnet den MAC $h_k(x)$ für einen ihm und dem Empfänger bekannten geheimen Schlüssel k und überträgt $x || h_k(x)$. Der Empfänger berechnet ebenfalls $h_k(x)$. Wenn die Werte übereinstimmen, ist die Nachricht authentisch, da ein Angreifer ohne Kenntnis von k keinen gültigen MAC bilden kann. HMAC [Krawczyk 1997] ist eine Möglichkeit, MACs aus Hashfunktionen zu konstruieren.

Auch **digitale Signaturen** dienen der Gewährleistung der Authentizität. Zusätzlich ermöglichen sie es dem Empfänger, gegenüber einem Dritten zu beweisen¹, daß der Sender die Nachricht signiert hat. Der Sender kann mit seinem privaten Schlüssel d und der Signierfunktion $S_d: \mathcal{M} \rightarrow \mathcal{C}$ (oder einem nichtdeterministischen Signieralgorithmus S_d) Signaturen für seine Nachrichten generieren. Mit dem zu d gehörigen öffentlichen Schlüssel e und der Verifikationsfunktion $V_e: \mathcal{M} \times \mathcal{C} \rightarrow \{\text{wahr, falsch}\}$ kann der Empfänger die Authentizität der signierten Nachricht prüfen.

Digitale Signaturen werden auch zur Zertifizierung öffentlicher Schlüssel eingesetzt, die dann auch über unsichere Kanäle ausgetauscht werden können. Der Anwender benötigt nur den öffentlichen Schlüssel einer vertrauenswürdigen Instanz, die mit ihrer Signatur die Zuordnung anderer öffentlicher Schlüssel zu Personen bestätigt.

¹Die Geheimhaltung der privaten Schlüssel ist dabei vorausgesetzt. Um zu verhindern, daß der Schlüsselhaber seinen geheimen Schlüssel verbreiten kann, wurden Chipkartenbasierte Verfahren vorgeschlagen.

3.2 Das ideale Modell der Anonymisierung

Im idealen Modell der anonymen Kommunikation existiert eine vertrauenswürdige Instanz, die Nachrichten anonymisiert weiterleitet. Jeder Teilnehmer verfügt über einen sicheren Kanal zur vertrauenswürdigen Instanz. Diese gibt die Nachrichten, die sie von den Teilnehmern erhält, anonymisiert weiter (*Sender-Anonymität*) und stellt Nachrichten an anonyme Adressen dem Empfänger zu (*Empfänger-Anonymität*). Da die Instanz vertrauenswürdig ist und es Angreifern weder möglich ist, die sicheren Kanäle abzuhören, noch sich über einen sicheren Kanal als die vertrauenswürdige Instanz auszugeben, ist das Senden und Empfangen von Nachrichten sowie die Beziehung von Sender und Empfänger unbeobachtbar. Somit erreicht dieses Verfahren perfekte Unbeobachtbarkeit und Anonymität. Alle ehrlichen (nicht mit dem Angreifer kooperierenden) Teilnehmer bilden die Anonymitätsmenge; über den Absender einer Nachricht ist nur bekannt, daß er dieser Menge angehört.

Der Angreifer kennt im idealen Modell die Nachrichten, die die mit ihm kooperierenden Instanzen gesendet haben. Nachrichten, die an eine mit dem Angreifer kooperierende Instanz gesendet oder an alle Teilnehmer verteilt werden, kann er beobachten und ggf. beeinflussen. Beobachtet der Angreifer eine ihm nicht bekannte Nachricht, muß somit einer der ehrlichen Teilnehmer der Absender sein. Jede dem Angreifer nicht bekannte anonyme Adresse muß einem der ehrlichen Teilnehmer gehören. Es ist nicht geheim, wer an dem Verfahren teilnimmt. Je weniger ehrliche Teilnehmer es gibt, desto größer ist die Wahrscheinlichkeit, daß der Angreifer eine anonyme Nachricht korrekt ihrem Absender zuordnet.

Ein reales Verfahren kann keine besseren Ergebnisse erzielen als das ideale [Micali 1992]; die Informationen, die der Angreifer im idealen Modell kennt, stehen ihm auch bei jedem realen Verfahren zur Verfügung.

Ein reales Anonymisierungsverfahren ist sicher, wenn es das ideale Modell mit kryptographischen Methoden so simuliert, daß ein Angreifer keine zusätzlichen Informationen gewinnen kann, obwohl keine physikalisch gesicherten Kanäle zur Verfügung stehen und keine einzelne Instanz als vertrauenswürdig feststeht [Beaver 1992, Goldreich 1997].

Ein sicherer Kanal kann simuliert werden, indem die Kommunikation zwischen zwei Instanzen so verschlüsselt wird, daß der Angreifer aus den abgehörten Nachrichten keine Informationen gewinnen kann. Wenn bei der Verschlüsselung die Länge der Nachrichten erkennbar bleibt, müssen zusätzlich bedeutungslose Nachrichten übertragen werden, um dem Angreifer keine Informationen darüber zu geben, ob Kommunikation stattfindet.

Eine vertrauenswürdige Instanz kann simuliert werden, indem mehrere Instanzen zusammenarbeiten, von denen zumindest ein Teil in Bezug auf eine bestimmte Funktion vertrauenswürdig ist. Den Teilnehmern muß dabei nicht bekannt sein, welche Instanzen tatsächlich die ehrlichen sind.

In realen Verfahren muß der Sender alle Nachrichten zusätzlich zu der in Anonymisierungsverfahren eingesetzten Verschlüsselung mit einem Schlüssel des Empfängers verschlüsseln, um die Vertraulichkeit der Inhaltsdaten sicherzustellen (Ende-zu-Ende-Verschlüsselung).

3.3 Das Mix-Netz

Ein **Mix** ist ein Netzknoten, der Nachrichten weiterleitet, wobei er den Zusammenhang zwischen seinen Ein- und Ausgaben durch Umkodieren verbirgt [Chaum 1981]. Wenn eine Nachricht eine *Sequenz* von unabhängigen betriebenen Mixen durchläuft, reicht es aus, daß einer der Mixe vertrauenswürdig ist, um Anonymität und Unbeobachtbarkeit der Kommunikationsbeziehung zu gewährleisten, auch wenn der Angreifer mit allen anderen Mixen kooperiert und sämtliche Kommunikationsverbindungen abhören kann. Realisiert werden Mixe durch den Einsatz asymmetrischer Verschlüsselung.

Hierdurch ergibt sich ein effizientes, gegen mächtige Angreifer sicheres Anonymisierungsverfahren. In seiner ursprünglichen Form ist das Mix-Netz insbesondere zur Übertragung von E-Mail geeignet; derartige Mixe werden auch als **Remailer** bezeichnet. Für interaktive Anwendungen muß das Verfahren modifiziert werden.

3.3.1 Anonymisierung von Nachrichten

Zu jedem Mix gehört eine Adresse M_j , ein öffentlicher Schlüssel e_j und ein privater Schlüssel d_j . Die Adressen und öffentlichen Schlüssel aller Mixe sind allen potentiellen Sendern bekannt. Will Sender A dem Empfänger B eine Nachricht m zukommen lassen, wählt er einen beliebigen Pfad $M_1, M_2, M_3, \dots, M_\lambda$ durch das Mix-Netz, wobei ein Mix auch mehrfach vorkommen kann, und bildet die Nachricht N_1 :

$$N_\lambda = E_{e_\lambda}(B || m)$$

$$N_i = E_{e_i}(M_{i+1} || N_{i+1}) \quad \text{für } i = \lambda - 1, \dots, 1$$

A sendet also $N_1 = E_{e_1}(M_2 || E_{e_2}(M_3 || E_{e_3}(\dots(E_{e_\lambda}(B || m))\dots)))$ an M_1 .

E ist dabei ein gegen aktive Angriffe sicherer probabilistischer Verschlüsselungsalgorithmus; $||$ bezeichnet die Konkatenation von Bitketten. Da Mixe beliebige Nachrichten automatisch entschlüsseln und das Ergebnis weiterleiten, ist Sicherheit gegen *chosen-ciphertext*-Angriffe erforderlich.

Mix M_j sammelt die empfangenen Nachrichten, bis hinreichend viele Nachrichten vorliegen. Für jede Nachricht berechnet er dann $D_{d_j}(N_j) = (M_{j+1} || N_{j+1})$ und sendet die resultierenden Nachrichten in veränderter Reihenfolge an den jeweils angegebenen Mix weiter. Der letzte Mix der Sequenz erhält $D_{d_j}(N_j) = (B || m)$ und sendet die Nachricht m an B.

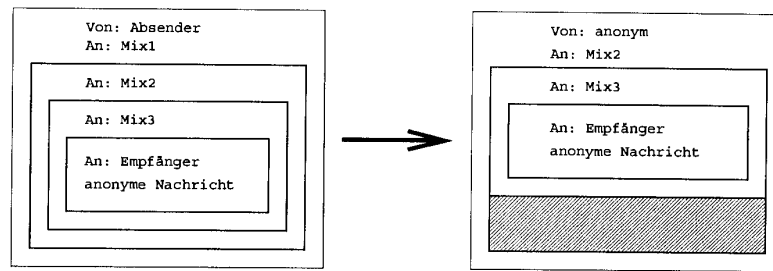


Abbildung 3.1: Anwendung einer Mix-Sequenz

3.3.2 Zuordbarkeit der Nachrichten

Für einen nicht mit M_j kooperierenden passiven Angreifer E sind die Nachrichten durch ihre *Länge*, durch die verschlüsselten – ohne Kenntnis der geheimen Schlüssel wie zufällig wirkenden – *Daten* und ihren *Ein- und Ausgangszeitpunkt* im Mix charakterisiert. Um Sicherheit gegen diesen Angreifertyp zu erreichen, muß verhindert werden, daß die Ein- und Ausgaben eines Mixes einander anhand dieser Merkmale zugeordnet werden können.

3.3.2.1 Umkodierung

Könnte der Angreifer eine Ausgabe mit größerer Wahrscheinlichkeit als durch zufälliges Auswählen einer Eingabe zuordnen, wären die Annahmen über das zugrundegelegte Kryptosystem verletzt [Rackoff 1993]. Einem Geheimtext, also der Eingabe eines Mixes sind ohne Kenntnis des Schlüssels keinerlei Informationen über den zugehörigen Klartext – die Ausgabe des Mixes – entnehmen, wenn das Kryptosystem sicher ist.

Umgekehrt ist es nicht möglich, den zu einem Klartext gehörenden Geheimtext zu identifizieren, weil die Verschlüsselung probabilistisch ist. Wenn allerdings ein Angreifer eine Nachricht aufzeichnet und mehrfach an den Mix sendet, ist die Voraussetzung, daß der Geheimtext zufällig ausgewählt wird, nicht erfüllt. Das wiederholte Senden identischer Eingaben (*Replay-Angriff*) an einen Mix führt zu identischen Ausgaben; damit kann ein aktiver Angreifer trivial feststellen, welcher Klartext zu einem beobachteten Geheimtext gehört. Um dies zu verhindern, muß der Mix Wiederholungen ignorieren.

3.3.2.2 Wiederholungen

Zum Erkennen von Wiederholungen kann der Mix ein eindeutiges oder jedenfalls nur mit vernachlässigbarer Wahrscheinlichkeit mehrfach auftretendes Merkmal jeder bearbeiteten Nachricht in einer Datenbank spei-

chern. Das Prüfen auf Wiederholung entspricht dann einem Datenbankzugriff. Da alle während der Gültigkeitsdauer eines Schlüsselpaares weitergeleiteten Nachrichten in der Datenbank vermerkt werden müssen, ist der Speicherplatzbedarf dieses Verfahrens groß. Wenn Nachrichten jeweils innerhalb eines bestimmten Zeitraums eintreffen, kann dieser Aufwand reduziert werden, indem der Absender den mit E_{e_j} verschlüsselten Teil der Nachricht mit einem Zeitstempel versieht. Der Mix akzeptiert dann nur Nachrichten mit gültigem Zeitstempel nach Abgleich mit der Datenbank [Gülcü 1996]. Da alte Nachrichten aufgrund ihres Zeitstempels ignoriert werden, können die entsprechenden Einträge in der Datenbank nach Ablauf der zulässigen Zeitspanne gelöscht werden.

Wenn der Zeitstempel den exakten Zeitpunkt der Nachrichtenerzeugung angibt, kann dies Rückschlüsse auf den Absender erlauben, die ansonsten aufgrund der Verzögerung durch die vorangegangenen Mixe nicht möglich wären. Um internen Angreifern hierdurch keine zusätzlichen Informationen zukommen zu lassen, sollte der Zeitstempel keine zu feine Auflösung haben. Um Rückschlüsse auf den tatsächlichen Erzeugungszeitpunkt zu verhindern, kann der Absender den Zeitstempel zudem um einen zufällig gewählten Wert zurückdatieren. Wenn die Zeitspanne, nach der die Datenbankeinträge gelöscht werden, größer ist als die tatsächliche Verzögerung der Nachrichten, hat die Rückdatierung keinen Einfluß auf die Gültigkeitsprüfung.

Als Merkmal zur Wiederholungsprüfung kann ein Hash-Wert der gesamten Nachricht verwendet werden. Auch wenn der Absender aus einem hinreichend großen Merkmalsraum eine *Message-ID* zufällig wählt, treten Kollisionen nur mit geringer Wahrscheinlichkeit auf.

3.3.2.3 Nachrichtenlänge

Bei der Entschlüsselung entfernt der Mix den Sitzungsschlüssel sowie die Adreßinformation aus dem Datenpaket. Die Nachricht wird dadurch kürzer. Sofern nicht für alle Nachrichten ein vorgegebener Pfad (*Kaskade*) verwendet wird, muß die Umkodierung *längentreu* erfolgen, um Angreifern keine Information über den Weg der Nachricht zu geben [Pfitzmann 1990]. Dazu ergänzt der Mix die Nachricht bis zur ursprünglichen Länge mit zufälligen Bits (*padding*). Da weder ein passiver Angreifer noch die folgenden Mixe – bei unverschlüsseltem m mit Ausnahme des letzten oder der mit ihm kooperierenden Mixe – die zur Entschlüsselung nötigen Schlüssel kennen, können sie das Padding nicht von verschlüsselten Nutzdaten unterscheiden. Um zu verhindern, daß die Padding-Länge nach dem Durchlaufen der Mix-Sequenz Informationen über die Länge des Pfades enthält, kann eine maximale Pfadlänge für das Gesamtsystem festgelegt werden. Die reservierten und nicht genutzten Einträge füllt dabei schon der Sender mit zufälligen Bits auf.

Durch diese Umkodierung werden die Nachrichten somit nach ihrer Länge in Klassen eingeteilt, innerhalb derer sie anonym und unbeobacht-

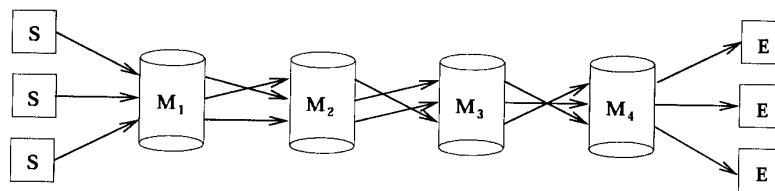


Abbildung 3.2: Schutz der Kommunikationsbeziehung durch eine Mix-Kaskade

bar sind. Um eine von der Nachrichtenlänge unabhängige Anonymitätsmenge zu erhalten, kann für alle Nachrichten eine einheitliche Länge festgelegt werden. Längere Nachrichten muß der Absender dann in mehrere Teile aufteilen; alle Nachrichten werden bis zur festgesetzten Länge mit zufälligen Bits aufgefüllt.

3.3.2.4 Umsortierung

Um die Unsicherheit über den Zusammenhang zwischen Ein- und Ausgabe zu erhöhen, müssen genügend viele Nachrichten gesammelt werden. Die Reihenfolge des Aussendens darf keine Informationen über die Reihenfolge des Empfangens der Nachrichten preisgeben. Für das Sammeln und Umsortieren der Nachrichten sind verschiedene Strategien möglich.

Im *Batch-Betrieb* sammelt ein Mix mindestens N Nachrichten an, die dann in beispielsweise lexikographischer Reihenfolge in einem Schub ausgegeben werden [Chaum 1981]. Im *Intervall-Batch-Betrieb* [Gülcü 1996] wird jeweils nach Ablauf eines festgelegten Zeitraums T ein Nachrichtenschub ausgegeben. Falls während des Intervalls nur $n < N$ Nachrichten eingetroffen sind, erzeugt der Mix $N - n$ bedeutungslose Nachrichten (*Dummies*). Damit ist T die maximale und $T/2$ die durchschnittliche Verzögerungszeit für eine Nachricht.

Für nicht interaktive Anwendungen sind weitere Strategien möglich. Bei *Stop-and-Go-Mixen* [Kesdogan 1998] legt der Absender die Verzögerung der Nachricht gemäß einer Exponentialverteilung zufällig fest. Um zu verhindern, daß durch zu frühes oder zu spätes Weiterleiten der vorhergehenden Mixe Angriffsmöglichkeiten entstehen, gibt der Absender zusätzlich ein *Zeitfenster* an, in dem die Nachricht eintreffen muß. Falls die Ankunftszeit außerhalb des Zeitfensters liegt, wird die Nachricht verworfen.

Im *Pool-Betrieb* wird, sobald die N -te Nachricht eintrifft, zufällig eine Nachricht ausgewählt und weiterverarbeitet [Franz 1997]. In diesem Fall ist die Verzögerung hinsichtlich eines Zählers, der jeweils beim Eintreffen einer neuen Nachricht erhöht wird, geometrisch verteilt: $P(\{T = k\}) = (1 - \frac{1}{N})^{k-1} \frac{1}{N}$. Der Erwartungswert ist $E(T) = N$, d. h. eine Nachricht bleibt im Durchschnitt bis zum Eintreffen N weiterer Nachrichten gespeichert.

Möglich ist auch der *Intervall-Pool-Betrieb*. In dieser Betriebsart wird jeweils nach Ablauf eines festgelegten Zeitraums geprüft, wieviele Nachrichten im Pool gespeichert sind. Enthält der Pool $n > N$ Nachrichten, werden nacheinander $n - N$ Nachrichten zufällig ausgewählt und bearbeitet. Andernfalls werden keine Nachrichten bearbeitet. In einer Variante mit *variabler Pool-Größe* werden in jedem Intervall nur $c(n - N)$ Nachrichten bearbeitet, $0 < c < 1$. Der Pool hat somit eine Mindestgröße; wenn mit gleichbleibender Häufigkeit Nachrichten eintreffen, ergibt sich für eine (möglicherweise größere) Poolgröße ein Gleichgewicht. Bei einem plötzlichen Ansteigen des Netzverkehrs wird der Pool größer.

Der Nachteil der poolbasierten Betriebsarten besteht darin, daß keine maximale Verzögerungszeit angegeben werden kann. Jedoch bleibt die Sicherheit des Verfahrens auch dann unverändert hoch, wenn wenige Nachrichten gesendet werden.

Ein Angreifer kann die Eingabe und die Ausgabe des Mixes beobachten. Anhand dieser Beobachtung kann er eine Nachricht mit einer Wahrscheinlichkeit \mathcal{G} korrekt dem Sender A zuordnen. Je größer die vom Mix erzielte *Konfusion*, desto kleiner ist \mathcal{G} .

In allen Betriebsarten beruht die Sicherheit des Mixes darauf, daß ausreichend viele Nachrichten gesammelt werden. Wird bei gleich vielen eintreffenden Nachrichten eine größere Anzahl von Nachrichten gesammelt, erhöht sich jedoch die Verzögerungszeit. Je mehr Nachrichten durch den Mix anonymisiert werden, desto mehr Nachrichten können gesammelt werden, ohne daß dadurch eine für den Nutzer inakzeptable Verzögerung auftritt.

3.3.3 Mix-Sequenzen

Wird mehr als ein Mix eingesetzt, erhöht sich die Zahl der geheimen Schlüssel, die kompromittiert werden müssen, um den Sender zu identifizieren.

Die Übertragungskapazität des zugrundeliegenden Kommunikationsnetzes kann besser ausgenutzt werden, wenn für alle Nachrichten ein fester Pfad vorgegeben ist, da dann keine Adreßangaben für die folgenden Mixe notwendig sind und es – da alle Nachrichten durch die Entschlüsselung gleichermaßen kürzer werden – nicht erforderlich ist, Nachrichten mit Padding aufzufüllen.

Da jeder Mix innerhalb der Kaskade nur Nachrichten von seinem Vorgänger erhält und an seinen Nachfolger sendet, ist das Mix-Netz einfacher zu verwalten und zuverlässiger, als wenn jeder Mix mit jedem anderen Nachrichten austauschen müßte [Gülcü 1996]. Auch ergeben sich kürzere Übertragungszeiten, da jeder Mix seinem Nachfolger einen bereits vollständigen Batch sendet.

Eine Mix-Kaskade mit Batchgröße N wird von N Nachrichten parallel durchlaufen. Somit ist die Wahrscheinlichkeit \mathcal{G} genauso groß wie bei

einem einzelnen Mix. Durch die Verwendung einer Kaskade erhöht sich also – sofern sie mehrere vertrauenswürdige Mixe enthält, die Sicherheit – nicht aber die Konfusion.

In einem System mit vielen Mixen ist es ineffizient, jede Nachricht durch alle Mixe zu senden. In dem Fall sollte der Nutzer die Möglichkeit haben, Mixe auf der Basis der Topologie des zugrundeliegenden Kommunikationsnetzes und seines Vertrauens zu wählen. Die Eingaben der Mixe sind dann voneinander verschieden. Die resultierende Konfusion kann daher bei gegebener Batchgröße größer sein als bei einem einzelnen Mix. In [Rackoff 1993] wird gezeigt, daß eine vor passiven Angreifern verborgene Permutation von n Nachrichten, also $\mathcal{G} = 1/n$, bei n Mixen der Batchgröße $N = 2$ bei in $\log(n)$ polynomiellen Pfadlängen erreicht werden kann.

In großen verteilten Mix-Netzen sind die meisten Betreiber dem Nutzer nicht bekannt; daher ist eine Auswahl nach Vertrauens Gesichtspunkten nicht sinnvoll. Es kann jedoch davon ausgegangen werden, daß jedenfalls ein Teil der Mixe vertrauenswürdige ist. Die Anonymität kann dann durch die zufällige Auswahl einer hinreichend großen Anzahl von Mixen gewährleistet werden. Wenn die verwendeten Mixe aus der Menge der vertrauenswürdigen zufällig ausgewählt werden, werden Angriffe durch die Unsicherheit über den jeweils verwendeten Pfad zusätzlich erschwert. Wenn ein Teil der Mixe nicht vertrauenswürdige ist, besteht bei zufälliger Auswahl jedoch das Risiko, einen Pfad auszuwählen, in dem keine vertrauenswürdigen Mixe enthalten sind. In dem Fall wäre die Anonymität des Nutzers im Einzelfall kompromittiert. Falls die Zugriffe des Nutzers verkettbar sind, hat ein solches Ereignis weitreichende Folgen. Die Vorteile beider Auswahlmethoden lassen sich kombinieren, indem festgelegte, vermutlich vertrauenswürdige Mixe in jedem Pfad verwendet werden, zusätzliche Mixe jedoch zufällig ausgewählt werden.

Im Intervall-Batch-Betrieb ergeben sich wie bei Mix-Kaskaden kurze Übertragungszeiten, da die Takte der aufeinander folgenden Mixe aufeinander abgestimmt werden können. Im ereignisgesteuerten Batch-Betrieb werden Nachrichten in jedem Mix verzögert. Der Erwartungswert der Verzögerungszeit steigt dabei proportional zur Pfadlänge.

3.3.4 Aktive Angriffe

Ein aktiver Angreifer kann Nachrichten unterdrücken und verfälschen. Gegen Angriffe durch verfälschte Nachrichten kann das Mix-Netz gesichert werden; Angriffe durch das Unterdrücken von Nachrichten sind nicht vollständig zu verhindern.

3.3.4.1 Verändern von Nachrichten

Vor dem Weiterleiten einer Nachricht prüft der Mix, daß er die jeweilige Nachricht noch nicht bearbeitet hat (Replay-Angriff, Abschnitt 3.3.2.2).

Möglicherweise kann ein Angreifer jedoch zu einer an den Mix gerichteten Nachricht weitere davon abgeleitete Geheimtexte erzeugen und an den Mix senden, ohne daß der Zusammenhang für den Mix zu erkennen ist. Wenn dieser die Eingaben in Ausgaben transformiert, die für den Angreifer erkennbar mit der echten Ausgabennachricht zusammenhängen, kann der Angreifer die zu der Nachricht gehörende Ausgabe identifizieren und so den Mix überbrücken. Bei einer direkten RSA-Implementierung von Mixen ist dieser Angriff möglich [Pfitzmann 1990b], nicht jedoch bei gegen *chosen ciphertext*-Angriffe sicherer Verschlüsselung.

Auch muß es unmöglich sein, Teile der Nachricht so zu ändern, daß sich das zur Prüfung auf Wiederholung (Abschnitt 3.3.2.2) verwendete Merkmal ändert. Der Mixmaster-Remailer [Cottrell 1995] verwendet für diese Prüfung eine 16 Bytes große *Message-ID*, die den Anfang des symmetrisch verschlüsselten Teils der Nachricht bildet. Da diese Verschlüsselung im CBC-Modus erfolgt, in dem ein Fehler im Geheimtext nur zu Fehlern im entsprechenden und dem darauffolgenden Klartextblock führt, bewirkt eine Verfälschung in den ersten acht Bytes, daß die entschlüsselte Nachricht eine andere *Message-ID* erhält, ansonsten aber identisch ist. Um diesen Angriff zu verhindern, muß der Mix die Integrität aller empfangenen Nachrichten prüfen.

Wenn, wie bei Verschlüsselung im ECB-Modus, identische Geheimtextblöcke zu identischen Klartextblöcken führen, ist ein aktiver Angriff durch Verfälschen von an Mixe gerichteten Nachrichten möglich: Der Angreifer dupliziert einen Block einer Nachricht an einer anderen Stelle und prüft, welche der Ausgabennachrichten das entsprechende Muster aufweist. Falls der Angreifer eine Nachricht verkürzt, indem er beispielsweise einen Teil des Paddings abschneidet, darf der Mix nicht eine entsprechend verkürzte umkodierte Nachricht ausgeben. Sonst könnte der Angreifer den Weg der Nachricht anhand ihrer Länge verfolgen.

Verhindert werden muß auch, daß ein Angreifer in einer Nachricht Informationen kodiert, die er nach dem Durchlaufen von Mixen der Ausgabenachricht wieder entnehmen kann, um Ein- und Ausgabe einander zuzuordnen. Statt des zufälligen Paddings könnte ein Mix von ihm gewählte Daten in eine Nachricht einfügen oder einen Teil der Nachricht durch von ihm gewählte Daten ersetzen. Informationen lassen sich auf diese Weise nicht in der Nachricht transportieren, da der erste ehrliche Mix der Sequenz die Nachricht mit einem dem Angreifer nicht bekannten Sitzungsschlüssel umkodiert; die Daten sind für den Angreifer nach der Umkodierung also nicht mehr lesbar. Das Verfälschen des Geheimtextes führt aber dazu, daß der zugehörige Klartext von der veränderten Position an nicht mehr lesbar ist; die resultierenden Daten sind pseudozufällig. Schon die Information, daß der Text an einer gegebenen Position verändert wurde, kann einem Angreifer die Zuordnung der Nachricht ermöglichen. Erkennen kann der Angreifer die Veränderung, wenn er den an den Empfänger gesendeten Klartext beobachtet, sowie in den Nachrichtenköpfen, die die mit ihm kooperierenden Mixe empfangen. Somit können ehrliche Mixe

überbrückt werden.

Diese Angriffe lassen sich verhindern, indem die Mixe die Integrität der von ihnen bearbeiteten Nachrichten anhand eines MAC prüfen. Im Nachrichtenkopf müssen dazu die vom Absender erzeugten MACs für die verschlüsselte Nachricht gespeichert sein. Wenn ein vom Mix berechneter MAC nicht dem vom Sender angegebenen entspricht, wurde die Nachricht verfälscht und muß verworfen werden. Diese Prüfung ist nicht möglich, wenn die Mixe zufällig erzeugtes Padding in weitergeleitete Nachrichten einfügen. Daher muß das Padding auf eine zwischen dem Absender und den jeweiligen Mixen vereinbarte Weise deterministisch erzeugt werden.

3.3.4.2 Deterministisches Padding im Mix-Netz

Wenn der Mix die als Padding einzufügenden Daten mit einem Pseudo-zufallszahlengenerator erzeugt, dessen Initialisierungswert vom Absender der Nachricht im jeweiligen Header vorgegeben wird, ist dem Absender die Form der Nachricht in jedem Schritt bekannt, und er kann entsprechende MACs erzeugen. Wenn die Nachricht den letzten Mix der Sequenz erreicht, enthält sie demzufolge die von allen vorangehenden Mixe eingefügten Padding-Daten in der Form, die durch „Entschlüsselung“ der Daten mit den jeweiligen Sitzungsschlüsseln entsteht, so daß der MAC von all diesen Daten abhängt.

Wenn der Nachrichtenkopf dem Nachrichtenkörper vorausgeht, hängt das Padding nach der Transformation durch die Entschlüsselungsfunktion seinerseits vom Inhalt der Nachrichtenköpfe – also von den verschlüsselten Sitzungsschlüsseln, MACs usw. – ab, da die Entschlüsselung in einem Modus erfolgen muß, in dem ein Geheimtextblock von allen vorangehenden Klartextblöcken abhängt (Abschnitt 3.1.1.1). Um dies zu verhindern, sollte der Nachrichtenkopf dem Nachrichtenkörper nicht vorangestellt werden, sondern ihm folgen. Alternativ dazu wäre es auch möglich, bei der symmetrischen Verschlüsselung der Nachricht in einem Feedback-Modus die Reihenfolge der Textblöcke umzukehren.

Bei der Erzeugung des MAC für einen Mix i muß die Form des Paddings, das von den Mixen 1 bis $i - 1$ eingefügt und durch Entschlüsselung umkodiert wird, bekannt sein. Dieses Padding muß der Absender zunächst durch wiederholte Verschlüsselung des Nachrichtenkörpers und darauf folgende Entschlüsselung des Nachrichtenkörpers mit dem jeweils bereits bekannten Padding erzeugen, bevor er die endgültige Form der Nachricht durch erneutes Verschlüsseln erzeugen kann. Dies ist möglich, da bei der ersten Verschlüsselungsoperation der Inhalt der Nachrichtenköpfe noch nicht bekannt sein muß, und auch bei der Entschlüsselungsoperation der Inhalt der für die Mixe i bis n bestimmten Nachrichtenköpfe für das Ergebnis keine Relevanz hat.

Für die Verschlüsselung der Nachricht m ergibt sich damit bei einer Mix-Sequenz der Länge n folgender Algorithmus:

- Erzeuge alle Sitzungsschlüssel k_i
- Verschlüssele den Nachrichtenkörper $N'_n := E_{k_n}(m)$
- Für Mix i von $n - 1$ bis 1:
 - Berechne die Nachrichtenkörper: $N'_i := E_{k_i}(N'_{i+1})$
- Setze $N_1^P := N'_1$
- Für Mix i von 1 bis $n - 1$:
 - Erzeuge durch Entschlüsselung die Nachricht mit Padding
 $N_i^P := D_{k_i}(N_{i-1}^P)$
- Setze $N_n := E_{k_n}(N_n^P) || MAC(N_n^P)$
- Für Mix i von $n - 1$ bis 1:
 - Erzeuge $N_i := E_{k_i}(N_{i+1}) || MAC(N_{i+1})$

3.3.4.3 Isolieren von Nachrichten

Ein Angreifer kann die von einem Mix erzielte Konfusion reduzieren, indem er eine große Anzahl von Nachrichten an den Mix sendet (*flooding*). Da er seine eigenen Nachrichten nach der Umkodierung wiedererkennt, besteht über diese Nachrichten keine Unsicherheit. Kennt er $N - 1$ der in einem Schub bearbeiteten N Nachrichten, ist die Zuordnung der N -ten Nachricht trivial. Daher sollte nach Möglichkeit verhindert werden, daß ein großer Teil der gleichzeitig bearbeiteten Nachrichten von einem Angreifer stammt.

Wie groß der Aufwand für einen *flooding*-Angriff ist, hängt von der Betriebsart der Mixe ab. Um eine bestimmte Nachricht zu verfolgen, kann der Angreifer sie abfangen und zusammen mit von ihm erzeugten Nachrichten an den Mix senden. Bei einer Mix-Kaskade im Batch-Betrieb muß er dafür $N - 1$ Nachrichten erzeugen, die dann zusammen mit der fraglichen Nachricht die Kaskade durchqueren. Bei einem frei wählbaren Pfad müssen in jedem Mix $N - 1$ Nachrichten vorliegen, wenn die Nachricht dort eintrifft. Der Angreifer muß daher insgesamt eine sehr große Zahl von Nachrichten erzeugen. Besonders viele Nachrichten muß der Angreifer im Intervall-Pool-Betrieb mit variabler Größe senden, bis alle in einem Mix gespeicherten Nachrichten von ihm stammen. Je mehr Nachrichten der Angreifer erzeugen muß, desto größer ist die Wahrscheinlichkeit, daß der Angriff entdeckt wird.

Eine weitere mögliche Maßnahme gegen das Isolieren von Nachrichten besteht darin, mit digitalen Signaturen sicherzustellen, daß die in einem

Schub bearbeiteten Nachrichten von verschiedenen Absendern stammen [Franz 1997]. Treffen zu viele Nachrichten von einem Absender ein, oder sind Nachrichten nicht mit einem von einem vertrauenswürdigen Dritten zertifizierten Signaturschlüssel signiert, lehnt der erste Mix diese Nachrichten ab. Die anderen Mixe können an dieser Stelle ebenfalls prüfen, um sicherzustellen, daß der erste Mix korrekt vorgeht. Mixe im Batch-Betrieb können mit einem Zero-Knowledge-Beweis zeigen, daß sie die Nachrichten protokollkonform umkodiert haben [Rackoff 1993].

Allerdings läßt sich, auch wenn mit kryptographischen Methoden sichergestellt wird, daß die gleichzeitig bearbeiteten Nachrichten von verschiedenen Absendern stammen, nicht feststellen oder verhindern, daß diese untereinander Informationen austauschen. Insbesondere in einem weltweiten offenen Netz, in dem die meisten Beteiligten den Mix-Betreibern nicht bekannt sind, bietet dieses Verfahren somit kaum Schutz.

Ein Mix kann die Unsicherheit über die zu einer Eingabe gehörende Ausgabenachricht erhöhen, indem er Dummy-Nachrichten erzeugt. Gegen den Empfänger der Nachricht bieten vom letzten vertrauenswürdigen Mix der Sequenz erzeugte Dummies keinen Schutz, da sie keine Unsicherheit über die Eingabe bewirken [Franz 1997].

Gibt ein vertrauenswürdiger Mix die umkodierten Nachrichten seinerseits unbeobachtbar aus, kann der Angreifer seine eigenen Nachrichten nicht mehr erkennen. Flooding-Angriffe werden dadurch wirkungslos. Sofern nicht alle Mixe gleichzeitig angegriffen werden, läßt sich dies erreichen, indem der Mix seine Ausgabe durch eine von ihm gewählte Mix-Sequenz weiterleitet (Umleitung, *Inter-Mix Detour*) [Gülcü 1996]. Wenn die von einem vertrauenswürdigen Mix ausgewählten Mixe mit dem Angreifer kooperieren, verursacht die Umleitung jedoch keine zusätzliche Unsicherheit über den Weg der Nachricht. Auch eine von einem mit dem Angreifer kooperierenden Mix trägt nicht zum Schutz der Nachricht bei.

Wenn ein Mix seine Ausgabe nicht nur an den nächsten Mix sendet, sondern an eine Gruppe von Mixen verteilt, kann der Angreifer den Weg der Nachricht nicht beobachten [Wayner 1996]. Sofern dem übertragenen Geheimtext keine Information über zu das verwendete Schlüsselpaar zu entnehmen ist, wird die Konfusion dadurch erhöht.

3.3.4.4 Unterdrücken von Nachrichten

Vereinfacht werden Flooding-Angriffe, wenn der Angreifer auch legitime Nachrichten unterdrücken kann. Außerdem ermöglicht das Unterdrücken von Nachrichten Angriffe gegen einzelne Teilnehmer.

Ein aktiver Angreifer, der den ersten Mix einer Kaskade oder den Übertragungsweg dorthin kontrolliert und die Ausgabe des letzten Mixes beobachten kann, kann Nachrichten isoliert in das Mix-Netz einspielen und die resultierende Ausgabe beobachten [Gülcü 1996]. Dieser zentrale Angriffspunkt existiert bei Mix-Netzen mit frei wählbarem Pfad nicht: Der

Sender kann eine Nachricht bei verschiedenen Mixen einliefern. Erzeugt er Nachrichten für verschiedene Mixe so, daß nach der Entschlüsselung durch einen Teil der Mixe für den letzten Teilpfad in beiden Fällen dieselbe Nachricht entsteht, erkennt der erste Mix dieses Teilpfads die Wiederholung und ignoriert die als zweite eintreffende Nachricht. Durch die redundante Übertragung wird ein höherer Aufwand zum Unterdrücken der Nachricht erforderlich.

Wenn der Nutzer vom ersten Mix eine signierte Empfangsbestätigung für die eingelieferten Nachrichten erhält, kann er nachweisen, daß seine Eingabe nicht korrekt bearbeitet wurde [Chaum 1981]; die Mixe zeigen mit einem Zero-Knowledge-Beweis ihr protokollkonformes Verhalten. Für den Pool-Betrieb ist keine maximale Verzögerungszeit festgelegt; daher kann dem Mix nicht nachgewiesen werden, daß er einen Angriff versucht hat [Franz 1997].

Es besteht jedoch auch die Gefahr, daß ein Nutzer aufgrund eines aktiven Angriffs oder auch eines Fehlers des zugrundeliegenden Kommunikationsnetzes keine Verbindung zu Mixen aufbauen kann. Die Möglichkeit, sich dagegen zu schützen, indem im Fehlerfall das gesamte Protokoll abgebrochen wird, ist bei einer großen Teilnehmerzahl nicht praktikabel.

Wenn der Angreifer Nachrichten eines Teilnehmers unterdrückt und zu einem späteren Zeitpunkt gesammelt an den Mix sendet, kann er aus den dann in entsprechend großer Zahl auftretenden anonymen Nachrichten auf die Zuordnung schließen. Die Wirksamkeit dieses Angriffs können Mixe durch das Prüfen eines Zeitstempels in der Nachricht einschränken.

3.4 Mix-Netze in interaktiven Anwendungen

Das Mix-Netz-Konzept ist besonders für die Versendung von E-Mail geeignet, für interaktive Anwendungen jedoch ineffizient. Da jeweils eine Nachricht vollständig übertragen und dann gegebenenfalls durch eine neue Nachricht beantwortet werden muß, sind viele asymmetrische Verschlüsselungsoperationen erforderlich. Bei kurzen Anfragen nimmt das erforderliche Padding einen großen Teil der Übertragungskapazität in Anspruch. Auch die Verzögerungen, die bei der anonymen Übertragung von Nachrichten durch ein Mix-Netz entstehen, sind für interaktive Dienste wie das WWW nicht akzeptabel.

Daher muß das nachrichtenbasierte Mix-Netz-Konzept für interaktive Anwendungen zu einem auf **anonymen Verbindungen** beruhenden Verfahren abgeändert werden. Um Verzögerungen bei der Nachrichtenübertragung zu verhindern, sind auch Kompromisse zwischen Sicherheit und Effizienz des Verfahrens nötig. Der Einsatz von *Mix-Kanälen* im Telefonnetz wurde in [Pfitzmann 1989] vorgeschlagen; eine Umsetzung für Internet-Dienste ist *Onion Routing* (Abschnitt 3.6.4). Bei diesem Verfahren bestehen Netzverbindungen zwischen Mixen, über die mit fester Rate

verschlüsselte Daten übertragen werden. Diese Netzverbindung wird im Multiplexverfahren für die anonymen Verbindungen genutzt; wenn keine Nutzdaten zu senden sind, wird Padding übertragen. Auf entsprechenden Prinzipien beruht auch der *PipeNet*-Vorschlag [Dai 1998].

3.4.1 Verbindungsaufbau

Der Sender wählt für seine anonyme Verbindung einen Pfad durch das Mix-Netz aus. Zwischen den aufeinander folgenden Mixen muß jeweils eine Netzverbindung bestehen.

Um eine anonyme Verbindung durch einen Mix aufzubauen, erzeugt der Sender eine Nachricht, in der die Adresse des folgenden Mixes oder des Empfängers sowie kryptographische Parameter für die anonyme Verbindung angegeben sind, und verschlüsselt sie mit dem öffentlichen Schlüssel des Mixes. Diese Nachricht wird als *Verbindungsaufbaunachricht* bezeichnet.

Ein Mix, der eine Verbindungsaufbaunachricht erhält, verknüpft die ankommende mit der abgehenden Netzverbindung zu einer anonymen Verbindung. Solange diese Verbindung besteht, werden über sie mit einer festen Rate verschlüsselte Daten übertragen. Die Verbindungsaufbaunachricht enthält symmetrische Schlüssel für die Übertragung von Daten in Hin- und Rückrichtung, für die Berechnung eines MAC und ggf. für die Erzeugung von Padding.

Im Onion-Routing-Verfahren enthält die Verbindungsaufbaunachricht die schichtenweise für die folgenden Mixe verschlüsselten Informationen; aufgrund dieser Form wird sie auch als *Onion* bezeichnet. Ihr Aufbau entspricht genau dem einer Nachricht im ursprünglichen Mix-Netz. In diesem Fall muß die Umkodierung der durch das Mix-Netz wandernden Verbindungsaufbaunachricht längentreu erfolgen.

Da der Verbindungsaufbau in diesem Fall bei allen Mixen unmittelbar nacheinander erfolgt, wird es internen Angreifern erleichtert, die Verbindung durch das Mix-Netz zu verfolgen. Es ist jedoch nicht erforderlich, die Verbindungsaufbaunachrichten für alle Mixe gleichzeitig zu übertragen. Stattdessen kann der Sender auch eine bereits bestehende anonyme Verbindung nutzen, um nach einer beliebig langen Verzögerung eine Verbindungsaufbaunachricht an den folgenden Mix zu senden.

Zum Erkennen vor Wiederholungen können Verbindungsaufbaunachrichten Message-IDs und Zeitstempel enthalten.

3.4.2 Anonyme Verbindung

Nachdem die anonyme Verbindung durch ein Mix-Netz aufgebaut ist, verschlüsselt der Sender die zu übertragenden Daten mit den symmetrischen Schlüsseln, die er beim Verbindungsaufbau mit den Mixen vereinbart hat.

Diese verschlüsselten Daten sendet er an den ersten Mix. Der Mix wartet, bis er auf allen anonymen Verbindungen je Richtung eine vorgegebene Menge von Daten empfangen hat; dann entschlüsselt er die vom anonymen Sender an den Empfänger gerichteten Daten und verschlüsselt die Antworten des Empfängers mit den in der Verbindungsaufbaunachricht angegebenen Schlüsseln und leitet die umkodierten Daten weiter. Nach der Weiterleitung und Anonymisierung durch das Mix-Netz erhält der Empfänger die Daten unverschlüsselt. Die Antworten erreichen den anonymen Nutzer in verschlüsselter Form; er entschlüsselt sie der Reihe nach mit den von ihm für den Rückkanal angegebenen Schlüsseln.

Tritt in einer anonymen Verbindung eine Verzögerung auf, führt dies somit zu einer entsprechenden Verzögerung bei allen Ausgaben des Mixes. Dies ist erforderlich, da Angreifer andernfalls anhand der Übertragungszeiten erkennen könnten, welche Ausgabe zu einer Eingabe gehört.

Das Verändern von Daten durch einen aktiven Angreifer würde dazu führen, daß unentschlüsselbare Daten an den Empfänger weitergeleitet werden. Da dies zur Identifizierung des anonymen Absenders führen könnte, müssen die Mixe die Authentizität der Daten anhand von durch den Sender erzeugten MAC prüfen. Schlägt die Prüfung fehl, müssen sämtliche anonymen Verbindungen abgebrochen werden, um dem Angreifer keine Informationen darüber zu geben, welche Ausgabe des Mixes zu der von ihm manipulierten Eingabe gehört. Es besteht die Gefahr, daß diese Maßnahme von maliziösen Sendern für *denial of service*-Angriffe mißbraucht wird. Diesem Problem kann begegnet werden, indem die Möglichkeit vorgesehen wird, im Fall einer fehlgeschlagenen MAC-Prüfung die betroffene Nachricht bis zu der Stelle zurückzuverfolgen, an der der Fehler aufgetreten ist.

In der Rückrichtung ist es nicht möglich, MACs durch die Mixe prüfen zu lassen. Hier kann nur der anonyme Nutzer selbst nach dem Entschlüsseln der Nachricht von den Mixen erzeugte MACs überprüfen.

3.4.3 Schutz vor Verkehrsanalyse

Da es jederzeit möglich sein soll, Verbindungen auf- und abzubauen, sind interaktive Mix-Netz-Varianten anfällig für Verkehrsanalyse.

Im Gegensatz zu den Nachrichten fester Länge im originalen Mix-Netz sind anonyme Verbindungen durch ihre Länge zu unterscheiden. Zudem ist es nicht möglich, Nachrichten zu sammeln und nach erst nach einer gewissen Verzögerung in geänderter Reihenfolge weiterzuleiten. Auch wenn die Übertragung paketweise erfolgt, müssen die Daten ohne nennenswerte Verzögerung weitergeleitet werden. Zudem sind die zu einer anonymen Verbindung gehörenden Pakete verkettbar. Um dies zu verhindern, müßte für jedes Paket ein neuer Pfad durch das Mix-Netz gewählt werden, was mit einem erheblichen Aufwand für die asymmetrische Verschlüsselung verbunden wäre. Aber selbst dann bleiben die Anfangs- und Endpunkt der

Pakete, die in direkter Folge gesendet und kurz darauf empfangen werden, gleich, so daß weiterhin Angriffe möglich sind.

Hat ein Mix, der nicht nur lokal von einem Nutzer verwendet wird, mehrere ehrliche Nachbarn, so ist für Angreifer nicht nachvollziehbar, ob ein Mix Daten weiterleitet, oder ob sie vom lokalen Nutzer stammen. Bei einem Mix, der über eine Telefonverleitung angebunden und daher nur temporär aktiv ist, ist jedoch unwahrscheinlich, daß er neben dem Eigentümer auch von anderen Anwendern genutzt wird.

Zum Schutz gegen Verkehrsanalyse muß daher Padding eingesetzt werden. Wenn sich die Menge der übertragenen Daten zwischen den Mixen und gegebenenfalls zwischen dem Nutzer und dem von ihm verwendeten Mix nicht in Abhängigkeit von den Nutzdaten ändert, können externe Angreifer nicht mehr beobachten, wann Verbindungen auf- und abgebaut werden oder wie viel Daten zu welchem Zeitpunkt übertragen werden. Dies läßt sich erreichen, indem das Datenvolumen mittels Padding auf eine konstante Größe gebracht wird. Anpassungen an die tatsächlich benötigte Kapazität sind möglich, wenn sie nicht in unmittelbarem zeitlichem Zusammenhang mit dem Auf- und Abbau anonymer Verbindungen erfolgen.

Wird das Padding auf den Verbindungen zwischen je zwei benachbarten Mixen eingefügt, sind passive externe Angriffe verhindert. Die Mixe selbst kennen in dem Fall jedoch die Menge der übertragenen Nutzdaten, so daß interne Angriffe möglich sind.

Ein aktiver Angreifer kann so viele anonyme Verbindungen aufbauen, bis die vorab festgelegte konstante Größe erreicht ist. Wenn das Mix-Netz dann weitere Verbindungen akzeptiert, ändert sich die Menge der übertragenen Daten wieder in Abhängigkeit von den Nutzdaten. Um aktive externe Angriffe zu verhindern, müssen weitere anonyme Verbindungen in diesem Fall also abgelehnt werden, oder das Datenvolumen muß so weit erhöht werden, daß wieder Padding eingefügt wird.

3.4.4 Schutz gegen interne Angreifer

Um sich gegen interne Angreifer zu schützen, muß Padding auf der anonymen Verbindung zwischen dem Nutzer und dem letzten von ihm verwendeten Mix eingefügt werden. Dadurch können die dazwischen liegenden Mixe keine zeitlichen Veränderungen der übertragenen Datenmengen beobachten.

Der Auf- und Abbau anonymer Verbindungen ist notwendigerweise allen beteiligten Mixen bekannt. Um zu verhindern, daß die Anonymität hierdurch kompromittiert wird, sollten die Zeitpunkte des Verbindungsaufbaus bei den verschiedenen Mixen eines Pfades möglichst weit auseinander liegen. Daraus folgt, daß der Nutzer nicht erst dann einen Pfad durch das Mix-Netz aufbauen sollte, wenn er tatsächlich anonym kommunizieren will. Stattdessen sollte er eine Verbindung durch das Mix-Netz

aufrechterhalten, wann immer das möglich ist. Die Zeitpunkte, zu denen der Pfad durch das Mix-Netz verlängert oder verkürzt wird, sollten zufällig gewählt werden, damit die einzelnen Schritte des Aufbaus einer anonymen Verbindung nicht verkettet und so einem einzelnen Nutzer zugeordnet werden können. Darüberhinaus ist es möglich, zufällig Verbindungen auf- und wieder abzubauen, auch wenn gar keine Daten gesendet werden sollen.

3.5 Anwendung für das WWW

Für die Akzeptanz der Nutzer ist es entscheidend, daß Anonymisierungsverfahren benutzerfreundlich realisiert werden. Die für anonyme Zugriffe notwendigen kryptographischen Operationen müssen durch ein vertrauenswürdiges System durchgeführt werden; die Kommunikation des Nutzers mit diesem System darf für Außenstehende nicht zu beobachten sein. Die nötige Software muß somit auf dem PC des Nutzers installiert werden.

Ein transparenter Zugriff über die gewohnte Benutzerschnittstelle ist möglich, indem der WWW-Browser des Nutzers die Anonymisierungs-Software als Proxy verwendet. Aufgabe eines solchen Proxies ist es neben der Durchführung kryptographischer Operationen auch, identifizierende Daten aus dem Dialog zwischen Browser und Server herauszufiltern.

Gelegentlich ist es auch wünschenswert, Informationen anonym anbieten zu können. Auch zu diesem Zweck können Mix-basierte Verfahren [Goldberg 1997, Demuth 1998] angewendet werden (Empfänger-Anonymität). Ein Angebot muß jedoch beliebig oft abgerufen werden können, so daß Replay-Angriffe (Abschnitt 3.3.2.2) nicht verhindert werden können. Ein gewisser Schutz gegen Angriffe ist durch den Einsatz von Proxy-Caches möglich, da Anfragen dann schon aus dem Cache beantwortet werden können und nicht bis zum anonymen Anbieter weitergeleitet werden müssen. Eine höhere Sicherheit ist gegeben, wenn der Anbieter seine Informationen anonym an einen Server überträgt, auf dem sie zum Abruf bereitgehalten werden, ohne daß der Betreiber des Servers die Identität des Anbieters kennen muß. Protokolle zur Anonymisierung von WWW-Zugriffen können so auch zum Schutz von Informationsanbietern eingesetzt werden.

3.6 Bestehende Systeme

Die meisten praktisch einsetzbaren Anonymisierungsverfahren sind Mix-Netz-basiert. Mit dem DC-Netz [Chaum 1988] existiert ein Verfahren, das informationstheoretisch sichere Sender-Anonymität gewährleistet, sofern die Schlüssel zufällig gewählt und über einen sicheren Kanal ausgetauscht werden und bei Schlüsselvereinbarung mittels asymmetrischer Verschlüsselung kryptographisch sicher ist. Der Aufwand für dieses Verfahren ist

jedoch sehr hoch, da alle Teilnehmer einen konstanten Strom verschlüsselter Daten senden und empfangen, wobei nur ein geringer Teil der Bandbreite für tatsächliche Kommunikation eingesetzt wird. Für den Einsatz in einem weltweiten Netz wie dem Internet ist dieses Verfahren daher nicht praktikabel.

Sofern darauf verzichtet wird, alle Teilnehmer in einer Anonymitätsmenge zusammenzufassen, können DC-Netze jedoch eingesetzt werden, um *lokale Anonymität* [Martin 1998] zu erzielen. Wenn die Benutzer anhand der Netztopologie in Gruppen eingeteilt werden, ist allerdings auch der Nutzen der Anonymisierung deutlich reduziert.

3.6.1 Crowds

Das *Crowds*-System [Reiter 1997] ermöglicht anonyme WWW-Zugriffe. Es bietet eine effiziente Möglichkeit, Anonymität gegenüber dem WWW-Server zu erreichen, wobei die Kommunikationsbeziehung für lokal abhörende Angreifer unbeobachtbar bleibt, schützt aber nicht gegen globales Abhören.

3.6.1.1 Verfahren

Der Nutzer ist Mitglied einer als *Crowd* bezeichneten Gruppe. Jeder Teilnehmer der *Crowd* betreibt einen *Jondo* genannten Prozeß. Um einen anonymen WWW-Zugriff durchzuführen, sendet der lokale Jondo die Anfrage an einen zufällig ausgewählten Jondo seiner Gruppe, möglicherweise an sich selbst. Ein Jondo, der eine Anfrage von einem anderen Teilnehmer empfängt, leitet sie mit Wahrscheinlichkeit p_f wiederum an einen zufällig ausgewählten Jondo weiter, andernfalls an den Server. Die Antwort des Servers wird auf dem so ausgewählten Pfad in der umgekehrten Richtung zum Nutzer übertragen. Die Kommunikation zwischen dem ersten und dem letzten Jondo wird mit einem vom Initiator erzeugten Schlüssel verschlüsselt, der in jedem Schritt verschlüsselt weitergegeben wird, also allen Beteiligten bekannt ist. Die weitergeleiteten Nachrichten werden von den Jondos nicht umkodiert.

3.6.1.2 Sicherheit

Für den WWW-Anbieter ist jedes Mitglied der *Crowd* als Sender gleich wahrscheinlich. Die Wahrscheinlichkeit, daß er den Zugriff dem Nutzer A korrekt zuordnet, ist $\mathcal{G} = \frac{1}{n}$. Würde der lokale Jondo sich nicht selbst auswählen, wäre $\mathcal{G} = \frac{1}{n-1}$, was bei kleinen *Crowds* nachteilig wäre.

Ein Angreifer, der die Kommunikation des Nutzers abhört, kann zwar feststellen, daß der Nutzer einen WWW-Abruf durchführt; wer der Empfänger ist, erfährt er aber nicht, da die Kommunikation mit den folgenden Jondos verschlüsselt wird. Wenn der Jondo des Nutzers den Zugriff je-

doch selbst durchführt, kann der Angreifer die unverschlüsselte Kommunikation mit dem Server beobachten. Zusätzlich erfährt er, daß der Jondo des Nutzers die Anfrage nicht von einem anderen Jondo erhalten hat und die Antwort nicht weiterleitet. Wenn der lokale Jondo sich, wie in [Reiter 1997], auch selbst auswählen kann, führt er den Zugriff mit Wahrscheinlichkeit $\frac{1-p_f}{n}$ selbst durch. Zusätzlich besteht die Möglichkeit, daß der zufällige Pfad im Jondo des Initiators endet. Dieser Fall ist für den Angreifer erkennbar, da die Nachrichten zwischen den Jondos nicht umkodiert werden.

Wenn der Anteil ehrlicher Teilnehmer um einen von p_f abhängenden Faktor größer ist als der der kompromittierten, dann ist es für interne Angreifer, der eine Anfrage erhält, wahrscheinlicher, daß der Jondo die Anfrage von einem anderen ehrlichen Jondo erhalten hat, als daß es sich um eine Anfrage des lokalen Nutzers handelt.

Gegen einen Angreifer, der mit einem der beteiligten Jondos kooperiert und zusätzlich die Kommunikationsverbindung des Nutzers abhören kann, bietet das Verfahren keinen Schutz. Dieser Angreifer kann feststellen, daß der Nutzer den Zugriff selbst veranlaßt hat und, da er den verwendeten Schlüssel kennt, auch die Kommunikation zwischen Nutzer und Server entschlüsseln.

Ein Angreifer, der die Kommunikation des Nutzers und die Kommunikation zwischen dem letzten Jondo und dem Server abhören kann, kann die unverschlüsselten Daten anhand ihrer Länge und der Zugriffszeit den verschlüsselten zuordnen. Auch in diesem Fall ist die Anonymität des Nutzers somit nicht gewährleistet.

3.6.2 JANUS

Das System JANUS [Demuth 1998] soll zum einen die Anonymisierung von Zugriffen auf WWW-Server ermöglichen, zum anderen aber auch das anonyme Anbieten von Informationen anhand verschlüsselter URLs, die vom JANUS-Server entschlüsselt werden.

Bei der Anonymisierung von WWW-Zugriffen entspricht die Sicherheit dieses Verfahrens nur der eines anonymisierenden Proxys: Die Verbindung zwischen dem Nutzer und dem JANUS-Server kann mit SSL verschlüsselt werden; personenbezogene Daten werden aus dem HTTP-Dialog entfernt. Eine Verkettung von JANUS-Servern ist jedoch nicht möglich. Die RSA-Verschlüsselung des JANUS-Systems dient ausschließlich dem Verschleiern der URLs anonymer Informationsanbieter.

3.6.3 Freedom

Freedom [ZKS 1999] ist ein kommerzielles Anonymisierungssystem der kanadischen Firma *Zero-Knowledge Systems, Inc.*, das an das Mix-Netz-Prinzip angelehnt ist.

3.6.3.1 Aufbau des Netzes

Das *Freedom*-Netz besteht aus Servern, die von verschiedenen Internet-Providern, Organisationen und Personen im Auftrag von *Zero-Knowledge Systems* betrieben werden.

Aufgabe dieser Server ist zum einen die Anonymisierung auf IP-Ebene, so daß TCP-Verbindungen, aber auch andere IP-basierte Protokolle anonymisiert werden können (*Anonymous Internet Proxy, AIP*), und zum anderen die Anonymisierung von E-Mail (*Anonymous Mail Proxy, AMP*).

Zusätzlich zu den Servern existiert eine zentrale Datenbank (*Freedom Network Information Database*), in der Informationen über die Topologie des Netzes sowie über Status und Performanz der einzelnen Server gespeichert sind, und ein *Keyserver*, der die öffentlichen Schlüssel der Freedom-Server und aller Pseudonyme enthält.

Jeder Freedom-Server hat fünf benachbarte Server; die Kommunikation zwischen benachbarten Servern wird mit einem gemeinsamen Sitzungsschlüssel verschlüsselt. In der Initialisierungsphase ruft ein Server die Schlüssel seiner Nachbarn aus der zentralen Datenbank ab, sofern sie nicht bereits vorliegen. Danach beginnt er, mit dem verbindungslosen *User Datagram Protocol (UDP)* Daten an seine Nachbarn zu senden. Wenn keine Nutzerdaten zu übertragen sind, werden Padding-Pakete gesendet. Durch einen *Traffic Shaper* wird das Padding so gewählt, daß eine vom Betreiber des Mixes vorgegebene maximale Bandbreite nicht überschritten wird; die übertragene Datenmenge ist unabhängig von der Menge der jeweils gesendeten Nutzdaten. Sie kann aber in Abhängigkeit von Statistiken über die zu erwartende Auslastung variieren.

Die Funktionsweise der *Anonymous Mail Proxies* ähnelt derjenigen herkömmlicher Remailer [Möller 1998]. Damit ist es möglich, E-Mail unter Pseudonym zu versenden und mit Hilfe von *Reply-Blocks* auch zu empfangen. Reply-Blocks sind vom anonymen Empfänger vorab erzeugte Nachrichten, in denen ein Pfad durch das Mix-Netz zum Empfänger kodiert ist. Während der Reply-Block bei der Weiterleitung durch das Mix-Netz entschlüsselt wird, wird die Antwort bei jedem Schritt mit einem vom Empfänger angegebenen symmetrischen Schlüssel verschlüsselt.

3.6.3.2 Client-Software

Eine auf dem Computer des Nutzers installierte Client-Software sorgt für transparenten anonymen Zugang zu den Netzdiensten DNS, HTTP, HTTPS, SMTP, POP3, Telnet, SSH, IRC (bis auf direkte Verbindungen zwischen Clients) sowie über ein WWW-Interface zum Usenet. über die Client-Software kann der Nutzer die Pfadwahl durch das Mix-Netz steuern und seine digitalen Pseudonyme verwalten.

Der Nutzer kann die Pfadlänge innerhalb bestimmter Grenzen auswählen; die voreingestellte Länge beträgt 3. Die Server können auf Wunsch

manuell ausgewählt werden, andernfalls wählt die Client-Software sie zufällig aus, wobei kein Server mehrfach verwendet wird und als erster ein dem Nutzer topologisch naher Server gewählt wird.

Als lokaler Proxy entfernt der Client personenbezogene Daten aus dem Datenstrom. Ausgehende Daten werden mit dem Schlüssel eines Pseudonyms signiert. Anhand dieser Signatur prüft *Freedom*, ob die anonyme Verbindung von einem berechtigten Nutzer stammt. Ein Nutzer erhält gegen Zahlung einer Gebühr die Berechtigung, eine bestimmte Anzahl von Pseudonymen zu verwenden [Lahey 1999]. Dadurch soll auch Mißbrauch verhindert werden, indem Pseudonyme bei mißbräuchlicher Verwendung gesperrt werden.

Anschließend werden die Daten über eine anonyme Verbindung durch das *Freedom*-Netz gesendet.

3.6.3.3 Anonyme Verbindungen

Ein *Freedom*-Server, der von einem Nachbarn ein Datenpaket empfängt, entschlüsselt zunächst mit dem gemeinsamen Schlüssel den Header des Pakets.

Handelt es sich um eine Verbindungsaufbaunachricht (*CREATE*), so wird sie mit dem privaten Schlüssel des Servers entschlüsselt. Verbindungsaufbaunachrichten enthalten einen *Anonymous Connection Identifier (ACI)*, die Adresse des folgenden Servers, Angaben über die zu verwendenden kryptographischen Algorithmen für die Hin- und Rückrichtung, die symmetrischen Schlüssel sowie eine Gültigkeitsdauer. Diese Daten werden für die Dauer der Verbindung gespeichert. Alle weiteren Pakete werden dann mit dem zur Verbindung gehörenden symmetrischen Schlüssel entschlüsselt.

Bei Nutzdaten-Paketen werden der Schlüssel und die kryptographische Operation (Ver- oder Entschlüsselung) anhand des ACI festgestellt. Nach der Umkodierung wird ein neuer Header erzeugt und das Paket an den folgenden Server weitergeleitet, wobei wiederum Verbindungsverschlüsselung eingesetzt wird. Der letzte vom Nutzer ausgewählte *Freedom*-Server leitet die Daten zum gewünschten Ziel weiter. Durch ein *DESTROY*-Paket wird die Verbindung wieder geschlossen.

3.6.3.4 Sicherheit des Verfahrens

Die *Freedom*-Software liegt nicht im Quellcode vor. [ZKS 1999] enthält nicht genügend Informationen über das Verfahren, um die Sicherheit beurteilen zu können.

Durch die obligatorische Verwendung von Pseudonymen besteht die Möglichkeit, anonyme Nutzer mit Kooperation der Server-Betreiber zurückzuverfolgen, da zu jedem Pseudonym drei *Reply-Blocks* gespeichert

sind, in denen jeweils ein Pfad durch das Mix-Netz zur Adresse des Nutzers kodiert ist. *Forward secrecy* ist somit aufgrund der mit temporären Sitzungsschlüsseln verschlüsselten Datenübertragung nur für die Vertraulichkeit der Nutzdaten gegenüber Außenstehenden gegeben, nicht aber in Bezug auf die Identität des Nutzers.

Da kein Padding nur auf den Verbindungen zwischen den Mixen eingesetzt wird, nicht aber zwischen dem Nutzer und den Mixen, ist Verkehrsanalyse durch interne und durch aktive externe Angreifer möglich (Abschnitt 3.4.3).

3.6.4 Onion Routing

Ein Onion-Routing-Netz [Reed 1998] besteht aus einer Anzahl von als *Onion-Router* bezeichneten Mixen, zwischen denen dauerhafte TCP-Verbindungen bestehen. Ein solches System befindet sich in dem Firewall, der das sichere Netz des Anwenders vom Internet trennt.

Der Zugriff auf das Onion-Routing-Netz erfolgt über *Anwendungs-Proxies*, so daß die Anonymisierung von Proxy-fähigen Anwendungen ohne Modifikation genutzt werden kann. Diese bestehen aus einem anwendungsspezifischen *Client-Proxy* und einem für das Onion-Routing-Protokoll zuständigen *Core-Proxy*. Die anonymisierte Verbindung endet in einem *Responder-Proxy*, der über eine TCP-Verbindung mit dem gewünschten Server kommuniziert.

Der Client-Proxy teilt dem Core-Proxy die Zieladresse mit und leitet Anfragen weiter, wobei er – sofern nicht nur Unbeobachtbarkeit, sondern auch Anonymität erreicht werden soll – identifizierende Daten wie Cookies entfernt. Gegebenenfalls erzeugt er anwendungsspezifische Fehlermeldungen. Client-Proxies existieren für HTTP, ftp, SMTP, und rlogin. Es ist auch möglich, mit einem IP-Tunnel beliebige Internet-Verbindungen zu anonymisieren.

Der Core-Proxy wählt einen Pfad durch das Onion-Routing-Netz, baut die Verbindung auf und leitet daraufhin die Daten vom Client-Proxy verschlüsselt an das Onion-Routing-Netz weiter.

3.6.4.1 Anonyme Verbindungen

Der Core-Proxy erzeugt eine Verbindungsaufbaunachricht („Onion“), die dem Mix-Protokoll entsprechend mehrfach verschlüsselt wird. Sie enthält für jeden Onion-Router eine Versionsnummer, Bezeichner für die Algorithmen, mit denen die Verbindung in Hin- und Rückrichtung verschlüsselt werden soll, die Adresse des folgenden Onion-Routers (oder 0, um den Responder-Proxy des Onion-Routers zu bezeichnen), die Gültigkeitsdauer der Verbindungsaufbaunachricht sowie einen Wert, aus dem die Sitzungsschlüssel abgeleitet werden. Im ersten Schritt wird zufälliges Padding angehängt; in den folgenden Schritten die für den jeweils nächsten Onion-

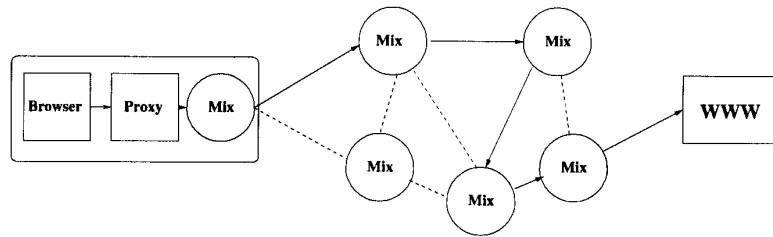


Abbildung 3.3: Anonyme Verbindung

Router bestimmte Nachricht. In Version 1 des Protokolls werden die ersten 1024 Bit der Nachricht direkt mit RSA verschlüsselt, die weiteren Daten mit DES im OFB-Modus. Die Pfadlänge ist auf 5 festgelegt. Für die Verbindungsverchlüsselung ist neben DES auch RC4 mit 128-Bit-Schlüsseln vorgesehen [Reed 1998]. Der beim Aufbau gewählte Pfad wird für die Dauer der gesamten Verbindung verwendet.

Ein Onion-Router, der eine Verbindungsaufbaunachricht erhält, entschlüsselt sie und prüft ihre Gültigkeit anhand der angegebenen Gültigkeitsdauer und eines Hash-Wertes, der zur Verhinderung von Replay-Angriffen gespeichert wird. Er erzeugt eine Datenstruktur, in der die ankommende und die ausgehende Verbindung sowie die Verschlüsselungssysteme für beide Richtungen miteinander verknüpft sind. Die Nachricht wird bis zu ihrer ursprünglichen Länge mit zufälligem Padding aufgefüllt und an den nächsten Onion-Router weitergeleitet.

Sobald die anonyme Verbindung besteht, können die mit den in der Verbindungsaufbaunachricht vereinbarten Schlüsseln stromchiffrierten Daten transportiert werden.

3.6.4.2 Verbindung zwischen Onion-Routern

Die Topologie des Netzes ist im voraus definiert. Jeder Onion-Router verfügt über DES-verschlüsselte Verbindungen zu einer festgelegten Menge von benachbarten Onion-Routern. Diese Verbindung wird im Multiplexverfahren für die anonymen Verbindungen sowie Steuerinformationen genutzt. Sie werden in *Zellen* fester Größe übertragen. Jede Zelle besteht aus einem für die betreffende dauerhafte Verbindung eindeutigen Bezeichner der anonymen Verbindung (*Anonymous Connection Identifier, ACI*), der Angabe ihres Typs, der Längenangabe der folgenden Nutzdaten sowie bis zu 44 Bytes Nutzdaten, die mit Padding auf die Maximallänge aufgefüllt werden. Es gibt Zellen der Typen *Padding*, *Create*, *Data* und *Destroy*.

Die Verbindungsaufbaunachrichten werden in *Create*-Zellen transportiert, die Nutzdaten in *Data*-Zellen. Wenn eine Verbindung abbricht, wird eine *Destroy*-Zelle mit der entsprechenden ACI übertragen, die der Empfänger an den folgenden Onion-Router weiterleitet und mit einer weiteren

Destroy-Zelle bestätigt; die zugehörigen Datenstrukturen werden dann gelöscht. Padding-Zellen werden eingefügt, um die Verkehrsanalyse zu erschweren; sie werden vom Empfänger ignoriert. Die Verbindungsver-schlüsselung wird für die bereits verschlüsselten Bestandteile der Create- und Data-Zellen ausgelassen.

Würde die Reihenfolge der ausgehenden Data-Zellen der der ankommenden entsprechen, wäre die Zuordnung der Verbindungen für einen Angreifer, der mit den benachbarten Onion-Routern zusammenarbeitet, trivial. Daher wird eine begrenzte Umsortierung vorgenommen: Zellen, die zu einem bestimmten Zeitpunkt von unterschiedlichen Onion-Routern gesendet wurden, können in beliebiger Reihenfolge weiterbearbeitet werden, ohne die Reihenfolge der Daten in einer Verbindung zu zerstören oder die Fairneß der Datenvermittlung zu beeinträchtigen. Solange diese Bedingungen erhalten bleiben, können mehrere Zellen einer Verbindung gesammelt und in geänderter Reihenfolge bearbeitet werden. Wenn zwischen interaktiven und nicht zeitkritischen Verbindungen unterschieden wird, bestehen bei letzteren verbesserte Möglichkeiten zur Umsortierung.

3.6.4.3 Sicherheit des Verfahrens

Zusätzlich zu den im einfachen Mix-Netz möglichen Angriffen sind bei Onion Routing einige weitere zu beachten.

Da die Verzögerung durch das Verfahren gering ist, wird die Verbindung zwischen Responder-Proxy und Empfänger nahezu gleichzeitig zur Verbindung zwischen Absender und Onion-Routing-Netz aufgebaut. Damit keine statistische Verkehrsanalyse möglich ist, muß die Kommunikationsverbindung zwischen dem Teilnehmer und seinem lokalen Onion Router also sicher sein, und der lokale Onion Router muß auch fremde Daten transportieren. Eine solche Konfiguration ist in vielen Fällen aber nicht gegeben [Reed 1998], insbesondere bei Privatanwendern.

Da die dauerhaften Verbindungen verschlüsselt und mit Padding aufgefüllt werden, ist die Verkehrsanalyse für externe Angreifer trotz der kurzen Verzögerungszeiten gegenüber dem einfachen Mix-Netz sogar erschwert. Die Nachbarn eines ehrlichen Onion-Routers können das Padding jedoch erkennen. Die Sicherheit gegen interne Angreifer ist also deutlich geringer. Für Onion-Router ist die Dauer einzelner Verbindungen zu erkennen. Kooperierende Onion-Router am Anfang und Ende einer anonymen Verbindung können die Anonymität daher auch aufdecken, wenn in der Verbindung zusätzlich ehrliche Onion-Router verwendet wurden. Sicherheit gegen diesen Angriff besteht, wenn der erste – definitionsgemäß vertrauenswürdige – Onion-Router ehrliche Nachbarn hat, so daß der Angreifer nicht feststellen kann, woher die Verbindung stammt. Auch in diesem Fall ist die erzielte Konfusion erheblich geringer als im Mix-Netz.

Die in [Reed 1998] vorgeschlagenen Verschlüsselungsverfahren sind nicht optimal: Um *forward secrecy* zu ermöglichen, sollte entgegen

[Reed 1998] Verbindungsverschlüsselung für alle Zellen eingesetzt werden. Anstelle direkter RSA-Verschlüsselung wäre ein Verfahren wie OAEP zu bevorzugen. Die Schlüsselgröße des verwendeten DES ist mit 56 Bit nicht ausreichend; für langfristige Sicherheit sollten RSA-Schlüssel mit mehr als 1024 Bit verwendet werden können.

3.7 Entwurf eines Protokolls

Onion Routing hat die meisten Eigenschaften, die für eine interaktive Mix-Netz-Anwendung sinnvoll sind. Einige Verbesserungen sind jedoch möglich. Wenn anonyme Verbindungen mittels einer mehrfach verschlüsselten *Onion* aufgebaut werden, kann ein interner Angreifer durch den zeitlichen Zusammenhang feststellen, wie sich diese Nachricht durch das Mix-Netz bewegt. Besser ist es, dem Client die Möglichkeit zu geben, die anonyme Verbindung schrittweise auf- und auch wieder abzubauen. Wenn der Client dabei verzögert vorgeht, ist dieser Angriff nicht mehr möglich.

Um sicherzustellen, daß die Datenübertragung zwischen zwei Mixen nicht vom tatsächlichen Kommunikationsaufkommen abhängt, kann die Verbindung zwischen den Mixen in Kanäle eingeteilt werden, wobei ein Kanal entweder einer anonymen Verbindung zugewiesen oder mit Padding aufgefüllt wird. Da eine anonyme Verbindung durch ihren Kanal identifiziert ist, ist die Übertragung von ACIs damit nicht mehr erforderlich.

Wenn des weiteren geeignete Verschlüsselungsalgorithmen eingesetzt werden und die Integrität der Daten anhand eines MAC sichergestellt wird, ergibt sich damit ein sehr sicheres Anonymisierungsverfahren mit vertretbarem Aufwand. Die konkrete Gestaltung eines solchen Verfahrens ist im folgenden Kapitel beschrieben.

Kapitel 4

Implementation

Bei der Anonymisierung von WWW-Zugriffen ist zwischen zwei Aufgaben zu unterscheiden: Ein *Client-Proxy* nimmt die HTTP-Requests des Browsers entgegen, entfernt daraus alle Daten, die den Nutzer identifizieren könnten und sendet den Request durch das Mix-Netz an den Server. Aus Antwort des Servers muß er wiederum alle Daten entfernen, die den Browser veranlassen könnten, die Identität des Nutzers – beispielsweise über ein nicht anonymisiertes Protokoll – zu offenbaren. Die anonyme und unbeobachtbare Verbindung zwischen dem Nutzer und dem Server wird dagegen vom *Mix-Netz* hergestellt.

4.1 Wahl der Programmiersprache

Damit das Anonymisierungssystem von vielen Nutzern verwendet werden kann und möglichst jeder Betreiber eines Internet-Servers, der das möchte, einen Mix betreiben kann, sollten sowohl der Proxy als auch der Mix auf den verbreitetsten Server-Betriebssystemen lauffähig sein. Ein Großteil der Server im Internet verwendet Unix-artige Systeme oder Windows NT. Es ist also sinnvoll, eine Programmiersprache zu wählen, die sowohl für Unix als auch für Windows NT vorhanden ist. Damit Nutzer den Proxy auf ihren privaten PCs installieren können, muß dieser auch unter Windows 95 lauffähig sein. Da das WWW interaktiv benutzt wird, muß die durch die Anonymisierung verursachte Verzögerung so gering sein wie möglich. Auch die Effizienz ist daher ein wichtiges Kriterium.

Perl ist auf vielen Unix-Systemen installiert; Windows NT wird ebenfalls unterstützt. Perl ist besonders für die schnelle Entwicklung kleinerer Programme geeignet. Nachteilig ist jedoch die geringe Ausführungsgeschwindigkeit.

Die Programmiersprache Java ist sehr portabel, und sowohl für Sockets als auch kryptographische Funktionen stehen Klassenbibliotheken zur

Verfügung¹. Java steht für Windows NT und auch für viele Unix-Systeme zur Verfügung. Obwohl neben Bytecode-Interpretern inzwischen auch Java-Compiler existieren, reicht die Effizienz von Java-Programmen noch nicht an die von C-Programmen heran.

C ist durch seine Maschinennähe sehr effizient und aufgrund seiner Hochspracheigenschaften gleichzeitig zur Entwicklung auch großer Programme geeignet. Nachteilig ist, daß die Speicherverwaltung zu großen Teilen dem Programmierer überlassen bleibt. Dies macht die Programmierung nicht nur aufwendig, sondern durch den daher notwendigen Umgang mit Zeigern sehr fehleranfällig. Viele Mängel der Sprache C sind in C++ [Stroustrup 1997] behoben. C++ erweitert C unter anderem um Möglichkeiten zur Datenabstraktion. Die Verwendung von Zeigern ist in vielen Fällen nicht mehr nötig; im Gegensatz zu Java sind Zeigeroperationen allerdings möglich. Bereichsprüfungen werden z. B. bei Zugriffen auf Vektoren nicht durchgeführt. Damit zusammenhängende Fehler werden wie in C nicht vom Compiler erkannt und sind auch zur Laufzeit teilweise nicht festzustellen.

Für Windows NT gibt es mehrere C++-Compiler. Der frei verfügbare Compiler GNU C++ wurde an eine Vielzahl von Unix-Systemen angepaßt und gehört zum Lieferumfang von beispielsweise Linux-Systemen. Bei der systemnahen Programmierung bestehen allerdings Unterschiede zwischen Windows NT und Unix. Wo es erforderlich ist, kann der für das jeweilige System vorgesehene Programmcode durch bedingte Kompilierung ausgewählt werden.

Kryptographische Funktionen gehören nicht zur Standardbibliothek von C++. Es gibt jedoch eine Reihe von Bibliotheken, die diese Funktionen zur Verfügung stellen. Weit verbreitet ist die Bibliothek OpenSSL, die Implementationen verschiedener kryptographischer Algorithmen vor C- und C++-Programme zur Verfügung stellt (Abschnitt 4.5).

Unix-Systeme stellen für die Kommunikation die *socket*-Schnittstelle zur Verfügung [Stevens 1998]. Damit ist es möglich, TCP-Verbindungen aufzubauen und wie auf Dateien lesend und schreibend auf sie zuzugreifen. Unter Windows wird diese Funktionalität mit geringen Abweichungen von der WINSOCK-Bibliothek zur Verfügung gestellt.

Für eine effiziente Implementation des Anonymisierungssystems ist C++ demnach in Verbindung mit OpenSSL eine geeignete Programmiersprache. Sie wird dem in dieser Arbeit entwickelten Code zugrundegelegt.

4.2 HTTP-Proxy

Ein anonymisierender HTTP-Proxy hat die Aufgabe, Anfragen von Browsern entgegenzunehmen und so weiterzuleiten, daß so wenig Informatio-

¹Aufgrund der Exportbeschränkungen für Verschlüsselungssysteme aus den USA gibt es neben der nur in den USA erhältlichen Java Cryptography Extension (JCE) auch eine international frei verfügbare Implementation namens IJCE.

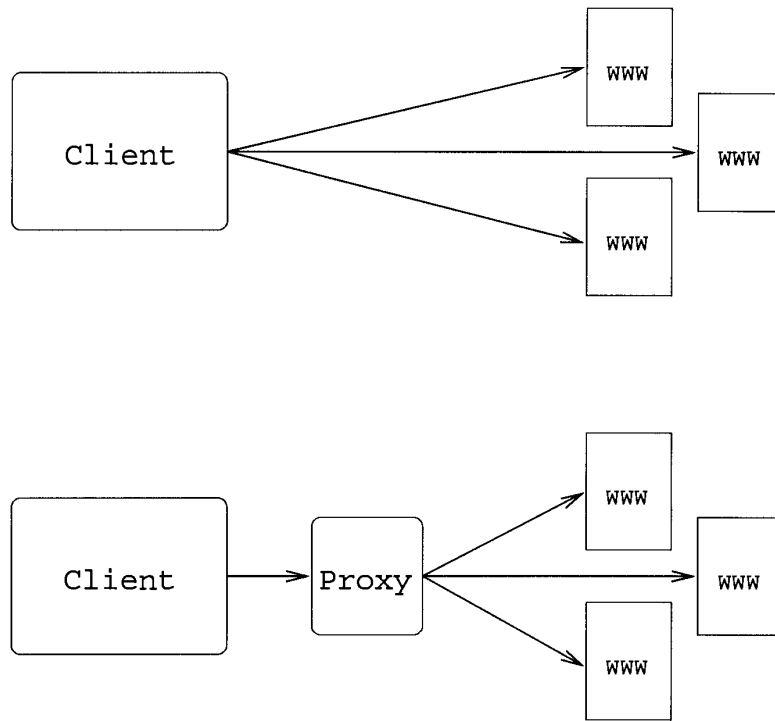


Abbildung 4.1: WWW-Zugriffe: direkt und über einen Proxy

nen über den Nutzer übermittelt werden, wie es möglich ist, ohne die Benutzbarkeit stark zu beeinträchtigen.

4.2.1 Request-Nachrichten

Ein Proxy agiert gegenüber dem Browser als ein HTTP-Server, für den eigentlichen Server hat er die Rolle eines Clients. Wenn der Proxy eine Anfrage erhält, sendet er eine entsprechende Anfrage an den Server.

Transparente Proxies leiten die Anfrage weitgehend unverändert weiter. Bestimmte Header-Zeilen, die sich nur auf die Verbindung zwischen Browser und Proxy beziehen, müssen gelöscht werden. Beim Zugriff auf den endgültigen Server ändert sich auch die Form des Request-URL, da HTTP/1.0-Server anstelle eines vollständigen URL nur die Pfad-Komponente (abs_path) [Berners-Lee 1998] erwarten.

Ein anonymisierender Proxy muß darüberhinaus weitere Header-Zeilen entfernen. Je nach Art der Header-Zeile können sich dabei Einschränkungen bei der Nutzung bestimmter WWW-Server ergeben.

Referer-Zeilen ermöglichen Analysen über das Verhalten der Nutzer und sollten daher nicht übertragen werden. Ebenso müssen From-Zeilen herausgefiltert werden, falls ein Browser sie erzeugt. Auch die Übertragung von Cookie-Headern [Kristol 1997] ist aus Datenschutzgründen nicht sinnvoll. Hiervon ausgenommen sind neuere Browser, die Cookies nur auf ausdrückliche Bestätigung des Nutzers anlegen.

User-Agent und weitere Browser-spezifische Header können es ermöglichen, Nutzer zu identifizieren, haben aber keine Bedeutung für die Anfrage selbst. Allerdings verwenden manche Server diese Zeilen, um auf bestimmte Browser abgestimmte Seiten zu übertragen. Die Unterdrückung solcher Header kann dann dazu führen, daß dem Nutzer Daten nicht angezeigt werden, obwohl sein Browser in der Lage ist, sie anzuzeigen. Daher kann es sich anbieten, eine fiktive Versionsangabe zu übertragen.

Die Header `Accept`, `Accept-Charset`, `Accept-Encoding` und `Accept-Language` übermitteln ebenfalls Informationen über den Nutzer. Die Liste der akzeptierten Datentypen ist nützlich, um Informationen optimal darstellen zu können. Da diese Möglichkeit relativ selten genutzt wird und in den meisten Fällen ein verbreitetes Format als Default ausgewählt wird, ist ihr Fehlen jedoch ein akzeptabler Nachteil. Das Fehlen des `Accept-Language`-Headers ist unproblematisch, da fast alle mehrsprachigen WWW-Server eine manuelle Auswahl der Sprache ermöglichen. `Accept-Encoding` ermöglicht die Auswahl von Transportkodierungen, insbesondere von Kompressionsverfahren. Wenn hierauf nicht verzichtet werden soll, könnte der Proxy selbst beispielsweise die `gzip`-Kompression unterstützen.

Der `Authorization`-Header ist unproblematisch, da er nur einen vom Nutzer selbst bewußt eingegebenen Namen und ein Paßwort enthält. Der Zugriff auf paßwortgeschützte Seiten ist somit unter einem Pseudonym möglich, wenn der Inhaltsanbieter es zuläßt.

Das Herausfiltern des Headers `If-Modified-Since` führt dazu, daß Seiten noch einmal übertragen werden, auch der Browser die aktuelle Version bereits gespeichert hat. Wird diese Zeile mitgesendet, werden jedoch auseinanderliegende Zugriffe eines Nutzers auf denselben Server verkettbar. Es ist daher sinnvoll, ihre Übertragung abhängig von den Sicherheitsbedürfnissen des Nutzers konfigurierbar zu machen.

Rückfragen an den Nutzer können auch sinnvoll sein, wenn der Proxy einen unbekanntem Header oder eine neue Zugriffsmethode feststellt, die zum Zeitpunkt der Implementation noch nicht bekannt waren.

4.2.2 Response-Nachrichten

Im Gegensatz zu Requests können die Antworten der WWW-Server ohne große Änderungen weitergeleitet werden.

Wenn Cookies herausgefiltert werden sollen, dürfen Set-Cookie und in anderen Versionen der Cookie-Spezifikation verwendete Varianten dieses Headers nicht an den Browser weitergeleitet werden. Wenn ein Cookie angelegt und nur bei der Anonymisierung der Anfragen nicht übertragen würde, könnten spätere nicht anonyme Zugriffe die Anonymität des Nutzers beim ursprünglichen Zugriff kompromittieren. Es reicht also nicht aus, nur die vom Browser an den Server übertragenen „Cookie“-Daten zu entfernen.

Wenn ein Browser Java oder JavaScript unterstützt, aber nicht die Möglichkeit gibt, diese Funktionalität zu deaktivieren, dann muß der Proxy entsprechende Elemente aus HTML-Dokumenten entfernen. Entsprechendes gilt für Hypertext-Links, die nicht anonymisierte Protokolle verwenden – insbesondere wenn sie durch das src-Attribut eines - oder <frame>-Tags automatisch ausgeführt werden.

4.2.3 Weitere Protokolle

ftp kann in gleicher Weise über einen Proxy verwendet werden wie HTTP. Wenn der anonymisierende Proxy das ftp-Protokoll nicht selbst unterstützt, kann er die anonymisierte Anfrage seinerseits an einen ftp-Proxy weitergeben.

Aus SSL-verschlüsselte Verbindungen zwischen Browser und Server können Proxies keine Daten herausfiltern. Es besteht jedoch die Möglichkeit, unverschlüsselte Daten an den Proxy zu senden, der dann die gesicherte Verbindung zum Server aufbaut.

4.2.4 Der filternde Client-Proxy AFproxy

AFproxy ist ein filternder HTTP-Proxy, der zum einen direkte Verbindungen zu Servern herstellen kann, und zum anderen den Übergang zu einem Mix-Netz bildet.

Die Mix-Netz-Software stellt eine Socket-basierte Schnittstelle zur Verfügung, über die ein Pfad durch das Mix-Netz gewählt und die Nutzdaten übertragen werden können (Abschnitt 4.3.6). AFproxy ist dafür zuständig, WWW-Zugriffe in gefilterter Form durch das Mix-Netz zu leiten. Aufgabe eines derartigen Client-Proxy kann es zusätzlich sein, dem Nutzer die Konfiguration des Anonymisierungssystems in Form eines HTML-Formulars zu ermöglichen.

AFproxy wird auf dem System des Anwenders installiert und akzeptiert daraufhin auf einem konfigurierbaren Port TCP-Verbindungen. Im WWW-Browser wird localhost mit der gewählten Portnummer als Proxy eingetragen. Daraufhin führt der Browser alle HTTP-Requests über diesen Proxy durch, sie verlassen das System des Anwenders also nur noch in

anonymer Form. Der Übergang zum Mix-Netz erfolgt über die in Abschnitt 4.3.6 beschriebene Schnittstelle. Der Client-Proxy wählt beim Programmstart einen zufälligen Pfad der vom Anwender vorgegebenen Länge durch das Mix-Netz. Alle anonymen WWW-Zugriffe der betreffenden Sitzung erfolgen dann über diesen Pfad.

4.3 WMix: Mix-Funktionalität

Ein Mix-Netz besteht aus einer Vielzahl von Knoten, den Mixen. Damit anonyme Zugriffe auf interaktive Dienste möglich sind, werden an Mixe die in Abschnitt 3.7 genannten Anforderungen gestellt. Das Programm WMix wurde entwickelt, um diese Mix-Funktionalität auf Unix- und Windows-Systemen zur Verfügung zu stellen.

Ein Nutzer, der das Mix-Netz nutzen möchte, installiert auf seinem Computer einen Client-Proxy (Abschnitt 4.2.4) und ebenfalls die Mix-Netz-Software WMix. Solange WMix aktiv ist, ist das System des Nutzers Teil des Mix-Netztes und kann jederzeit anonyme Verbindungen initiieren.

4.3.1 Konfiguration

Bestimmte Daten für die Konfiguration der Mixe werden im voraus festgelegt. Beim Aufbau einer anonymen Verbindung dient eine Liste in der alle aktiven Mixe mit ihrem Host-Namen, der Portnummer und ihrem öffentlichen Schlüssel verzeichnet sind, zur Wahl eines Pfades durch das Mix-Netz. Eine solche Liste kann über das WWW verbreitet werden.

Jeder Mix-Server hat eine Konfigurationsdatei, aus der hervorgeht, von welchen Servern und gegebenenfalls welchen Anwendern Verbindungen akzeptiert werden, und ob der Mix anonyme Verbindungen zu externen Servern durchführt. Außerdem ist in dieser Datei festgelegt, zu welchen anderen Servern der Mix auf welchem Port eine Verbindung aufbaut. In dieser Datei können auch symmetrische Schlüssel für die gesicherte Datenübertragung zwischen den Mixen angegeben und die für die Verbindung vorgesehene Bandbreite festgelegt werden.

4.3.2 Schlüsselverwaltung

Voraussetzung für die Sicherheit der asymmetrischen Verschlüsselung ist, daß die verwendeten öffentlichen Schlüssel zertifiziert werden. Geeignete Zertifizierungsinfrastrukturen stehen im Internet zur Verfügung; die derzeit verbreitetste ist PGP [Callas 1998]. Da WMix ebenso wie PGP RSA-Schlüssel verwendet, wäre es möglich, die öffentlichen Schlüssel der Mixe im PGP-Format zu speichern und entsprechende Zertifikate zu erzeugen. Eine flexiblere Lösung besteht jedoch darin, die Schlüssel als Textdatei zu signieren. Das WMix-Schlüsselformat bleibt dadurch unabhängig

von der zur Zertifizierung verwendeten Software. Der Betreiber eines Mixes erzeugt einen PGP-Schlüssel, mit dem er den WMix-Schlüssel signiert; die Authentizität des PGP-Schlüssels wird durch das PGP-*web of trust* gewährleistet.

4.3.3 Algorithmen

Für die Implementation wurden als sicher geltende kryptographische Algorithmen (Abschnitt 3.1) ausgewählt. Die Verwendung der Algorithmen wird jeweils beim Verbindungsaufbau ausgehandelt, so daß die Auswahl der Algorithmen leicht an neue Erkenntnisse über die Sicherheit von Verschlüsselungsverfahren angepaßt werden kann. Zur asymmetrischen Verschlüsselung wurde RSA im OAEP-Modus mit 1024-Bit-Schlüsseln ausgewählt. Der symmetrischen Verschlüsselung dient Triple-DES mit 112-Bit-Schlüsseln und einem Initialisierungswert von 8 Bytes im *CBC*-Modus; die Integrität der Daten wird mit Hilfe von HMAC-SHA-1 gewährleistet. Damit ein Paket-Header einschließlich eines Typ-Bytes nicht mehr als 16 Bytes umfaßt, wird die Variante HMAC-SHA-1-120 eingesetzt, so daß der Hash-Wert nur 15 Bytes groß ist. Bei der Berechnung des MAC wird den eigentlichen Daten eine Sequenznummer des jeweiligen Pakets als Zwei-Byte-Wert vorangestellt, um zu verhindern, daß Pakete vertauscht werden können.

Die Ausgabe des Padding-Algorithmus soll ohne Kenntnis des geheimen Schlüssels nicht von Zufallsdaten zu unterscheiden sein. Falls der Algorithmus dieses Ziel nicht erreicht, erhalten Angreifer nur die zusätzliche Information, ob ein Data-Paket vom absendenden Mix weitergeleitet oder aber von einem lokalen Nutzer erzeugt wurde. Da lokale Nutzer eine Sequenz aus mehreren anderen Mixen verwenden, ist diese Information nicht sehr sensitiv. Als effizienter Algorithmus wird für diesen Zweck in WMix der auf einer Hashfunktion beruhende Algorithmus MGF1 [Kaliski 1998] verwendet.

Die verwendeten kryptographischen Algorithmen werden durch numerische Bezeichner repräsentiert. Folgende Algorithmen sind definiert:

NULL	0
RSA	1
NULL	0
3DES	1
NULL	0
HMAC-SHA-1	1
NULL	0
MGF1	1

Ist ein Verschlüsselungsalgorithmus NULL, werden die Daten unverschlüsselt übertragen. Für die MAC- und Padding-Algorithmen bedeutet

NULL, daß alle Ausgabebytes den Wert 0 haben. Die NULL-Algorithmen werden nur beim Verbindungsaufbau eingesetzt, bis die Kommunikationspartner mit Hilfe von `SessionKey`-Paketen Algorithmen und Schlüssel für ihre Verbindung vereinbart haben.

4.3.4 Verbindung zwischen zwei Mixen

Zwischen den Mixen bestehen langfristige Socket-Verbindungen. Das Protokoll wird in Runden ausgeführt; in jeder Runde senden alle Mixe jeweils eine feste Anzahl von *Paketen* vorgegebener Länge. Somit wird eine Verbindung durch Multiplexen für mehrere zur anonymen Kommunikation dienende *Kanäle* genutzt. Benachbarte Mixe vereinbaren die Anzahl der zwischen ihnen bestehenden Kanäle; die Zahl kann im laufenden Betrieb angepaßt werden, so daß immer ausreichend viele Kanäle zur Verfügung stehen, um neue anonyme Verbindungen aufbauen zu können. In nicht genutzten Kanälen wird Padding übertragen.

Sofern die Betreiber nichts anderes vereinbart haben, wird unmittelbar nach dem Aufbau einer Verbindung in jeder Runde ein Paket gesendet; die Verschlüsselungs- und Authentisierungsalgorithmen sind NULL. Die Kommunikationspartner können die Verschlüsselungsparameter und die Anzahl der Pakete je Runde aushandeln, indem sie `SessionKey`-Pakete austauschen. Der die Verbindung aufbauende Mix sendet zunächst `Padding`-Pakete, bis der andere Mix seine Konfigurationsdaten übertragen hat. Solange die Verbindung ungesichert ist, werden nur `Padding`-Pakete und `SessionKey`-Pakete für die Vereinbarung eines geheimen Schlüssels gesendet.

Da ein Mix die Bearbeitung der empfangenen Pakete erst beginnen kann, wenn er alle Pakete der jeweiligen Runde erhalten hat, ist die Geschwindigkeit des Netzes durch den langsamsten Knoten bestimmt. Die Bearbeitung erfolgt daher mit höchster Priorität, um die maximal mögliche Geschwindigkeit zu erreichen. Da das Programm durch einen `select`-Aufruf solange angehalten werden kann, bis auf einem der benutzten Sockets Daten zum Lesen bereitstehen, führt dieses Vorgehen nicht zu einer übermäßigen Auslastung der beteiligten Systeme.

4.3.5 Pakete

Ein Paket ist 256 Bytes groß. Folgende Typen sind definiert:

Padding	1	Data	9
Create	2	RData	10
Connect	3	Userdata	11
ApplConnect	4	RUserData	12
Close	5	CreateAck	13
Closed	6	Error	14
ApplClose	7	SessionKey	15
RApplClosed	8	ReqChannel	16

Die Pakete haben folgenden Aufbau:

Byte	0:	Längenangabe
Bytes	1–127:	Nutzdaten + Padding
Bytes	128–239:	Padding
Byte	240:	Typ
Bytes	241–255:	MAC

Der Nachrichtenkopf bildet also, wie in Abschnitt 3.3.4.2 begründet, das Ende des Pakets. Für Pakettypen, die Daten variabler Länge enthalten können, ist Byte 128 die Längenangabe; die eigentlichen Nutzdaten sind in den Bytes 129–255 enthalten. Andere Pakete, wie etwa `AppClose` enthalten keine Nutzdaten; Byte 0 hat dann den Wert 0.

Das Padding (Bytes 128–239) ermöglicht es, Pakete längentreu umzukodieren, um sie durch das Mix-Netz zu transportieren. Es wird in die Berechnung der MACs einbezogen, ist aber ansonsten bedeutungslos. Dadurch können Pakete in `Data`- und `RData`-Paketen gekapselt werden können. Damit alle Pakettypen gleich behandelt werden können, ist dieses Padding auch bei Paketen vorhanden, die nicht in anonymisierter Form durch das Mix-Netz übertragen werden.

`Data`- und `RData`-Paketen haben folgenden Aufbau:

Byte	0:	Längenangabe
Bytes	1–127:	Nutzdaten + Padding
Bytes	128–239:	Steuerinformationen für weitere Mixe
Byte	240:	Typ
Bytes	241–255:	MAC

Die Nutzdaten einschließlich Längenangabe und Padding sind dabei verschlüsselt. Bei den Steuerinformationen handelt es sich um aus Typangaben und MACs bestehende Abschnitte, die in der umgekehrten Reihenfolge des Pfades in verschlüsselter Form vorliegen.

Um Modifikationen an Paketen entdecken zu können, enthält jedes Paket eine *Message Authentication Code*. Der MAC richtet sich nach dem zwischen den Mixen vereinbarten Algorithmus und dem hierfür vereinbarten geheimen Schlüssel, bei über eine anonyme Verbindung übertragenen Paketen nach den in der Verbindungsaufbaunachricht angegebenen Parametern.

Wird ein Paket mit ungültigem MAC empfangen, muß der Mix es ignorieren und zur Verhinderung von Angriffen alle aktiven anonymen Verbindungen unterbrechen. Dies gilt auch für `Padding`-Pakete, da diese für Angreifer nicht von Daten zu unterscheiden sein dürfen.

Zusätzlich zur der für eine anonyme Verbindung zwischen dem Nutzer und dem jeweiligen Mix vereinbarten Verschlüsselung werden alle über die `Socket`-Verbindung zwischen zwei Mixen übertragenen Daten symmetrisch verschlüsselt. Der MAC wird geprüft, nachdem das empfangene Paket mit dem zur `Socket`-Verbindung gehörenden und gegebenenfalls mit dem vom Absender angegebenen Schlüssel dechiffriert wurde.

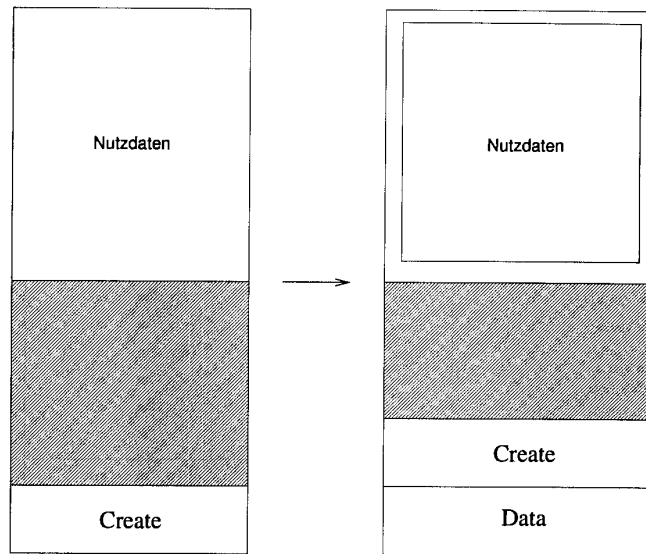


Abbildung 4.2: Create-Paket in einem Data-Paket

4.3.5.1 Padding

Padding-Pakete werden ignoriert. Sie dienen dazu, unabhängig vom tatsächlichen Kommunikationsaufkommen einen konstanten Datenstrom zu senden (siehe Abschnitt 3.4.3).

4.3.5.2 SessionKey

Nach dem Aufbau einer neuen Verbindung zwischen zwei Mixen wird ein `SessionKey`-Paket verwendet, um Algorithmen und Sitzungsschlüssel zu vereinbaren. Es enthält Schlüssel für die Ver- und Entschlüsselung sowie für die Überprüfung von MACs in beiden Richtungen.

Der Inhalt des Pakets ist mit dem öffentlichen Schlüssel des empfangenden Mixes verschlüsselt. Die Daten sind damit nur den beteiligten Mixen bekannt. Das Paket wird vom absendenden Mix nicht authentisiert; *man in the middle*-Angriffe auf das Mix-Netz sind dennoch nicht möglich, da die nachfolgenden Verbindungsaufbaunachrichten jeweils nur vom ausgewählten Mix entschlüsselt werden können.

4.3.5.3 ReqChannel

Ein Mix kann ein `ReqChannel`-Paket erzeugen, wenn die Bandbreite der Verbindung zu einem Nachbarn nicht ausreicht. In der auf das `ReqChannel`-Paket folgenden Runde ist die Anzahl der Kanäle dieser Verbindung um eins erhöht. Dies sollte nicht automatisch beim Aufbau neuer

anonymer Verbindungen geschehen, da der Angreifer dann aus der Erhöhung der Anzahl von Kanälen auf den Verbindungsaufbau zurückschließen könnte. Stattdessen kann die Anpassung der Bandbreite in bestimmten Zeitabständen oder zu zufällig gewählten Zeitpunkten erfolgen. Die Mixe können ein Maximum an Kanälen vereinbaren; wenn sämtliche Kanäle durch anonyme Verbindungen belegt sind, können keine weiteren anonymen Verbindungen aufgebaut werden. Indem die Anzahl der Kanäle durch ReqChannel-Pakete erhöht, aber nur durch den Neustart des Systems reduziert werden kann, wird verhindert, daß Angreifer aus einer Reduzierung der Kanäle auf die Anzahl der bestehenden anonymen Verbindungen schließen kann.

4.3.5.4 Create

Eine Verbindungsaufbaunachricht wird dem Mix in einem oder mehreren Create-Paketen übermittelt. Hat die Längenangabe des Pakets den Wert 255, bedeutet das, daß die Nachricht im folgenden Create-Paket fortgesetzt wird; ansonsten gibt sie an, wieviele Bytes folgen.

Die Verbindungsaufbaunachricht beginnt mit einem Byte, das den verwendeten asymmetrischen Algorithmus angibt; die folgenden Daten sind asymmetrisch verschlüsselt. Der verschlüsselte Datenblock enthält Angaben der Algorithmen sowie die Schlüssel für die Verschlüsselung des Datenstroms in Hin- und Rückrichtung sowie zur Bildung der MACs und des Paddings für beide Richtungen. Zum Schutz gegen Replay-Angriffe kann der Mix einen Hash-Wert des Pakets speichern; als Zeitstempel ist das Erzeugungsdatum im Create-Paket enthalten.

Im OAEP-Modus können mit RSA bei Verwendung von 1024-Bit-Schlüsseln bis zu 86 Bytes verschlüsselt werden. Diese Größe wird bei der vorliegenden Implementation nicht überschritten. Bei größeren Verbindungsaufbaunachrichten müßten die darüberhinausgehenden Daten mit einem im RSA-verschlüsselten Teil enthaltenen Sitzungsschlüssel symmetrisch verschlüsselt werden.

Ein Mix, der eine Verbindungsaufbaunachricht erfolgreich entschlüsselt und für die neue anonyme Verbindung einen Kanal reserviert hat, bestätigt dies mit einem CreateAck-Paket. Nach dem Senden des CreateAck-Pakets werden die neu vereinbarten Sitzungsschlüssel verwendet. Während der Entschlüsselung darf die Datenübertragung nicht unterbrochen werden; falls die kryptographische Operation sehr zeitaufwendig ist, muß sie also in einem separaten Thread durchgeführt und auf dem betreffenden Kanal währenddessen Padding-Pakete übertragen werden. Andernfalls wäre durch die Verzögerungen für externe Angreifer zu erkennen, wie durch das Mix-Netz eine anonyme Verbindung aufgebaut wird.

4.3.5.5 CreateAck

CreateAck-Pakete enthalten lesbaren Text. Die erste Zeile enthält den Namen des Mixes, der die Verbindung bestätigt. Darauf folgen jeweils in einzelnen Zeilen die Namen aller benachbarten Mixe, zu denen dieser Mix eine anonyme Verbindung aufbauen kann.

4.3.5.6 Error

Ein Error-Paket wird erzeugt, wenn ein Fehler aufgetreten ist, beispielsweise eine gewünschte anonyme Verbindung nicht aufgebaut werden konnte. Der Inhalt dieses Pakets ist eine Beschreibung der Fehlersituation in natürlicher Sprache.

4.3.5.7 Connect

Ein Paket dieses Typs enthält den Namen des Mixes, zu dem eine anonyme Verbindung aufgebaut werden soll. Üblicherweise besteht der Name eines Mixes aus seinem Domainnamen und, getrennt durch einen Doppelpunkt, der Portnummer.

Nachdem der Mix für die anonyme Verbindung einen Kanal belegt hat, ist dieser ausgehende Kanal für die Dauer der Verbindung dem Kanal zugeordnet, auf dem der Mix das Connect-Paket erhalten hat.

4.3.5.8 ApplConnect

Ein ApplConnect-Paket teilt dem empfangenden Mix mit, daß eine TCP-Verbindung zu einem WWW-Server oder einem anderen Internet-Dienst aufgebaut werden soll.

Hat die Längenangabe der Nutzdaten den Wert 0, dann baut der Mix eine Verbindung zu seinem vorgegebenen HTTP-Proxy auf. Andernfalls besteht die Adresse aus dem Hostnamen und, getrennt durch einen Doppelpunkt, der Portnummer des gewünschten Dienstes. Ein Mix muß nicht alle Netzdienste unterstützen; Beschränkungen sind sinnvoll, um keine Angriffe auf andere Systeme durch anonymes *remote login* zu ermöglichen.

4.3.5.9 ApplClose, RApplClosed

Mit einem Paket des Typs ApplClose wird der empfangende Mix aufgefordert, die TCP-Verbindung zu schließen. Die anonyme Verbindung bleibt dabei jedoch bestehen und kann zum Aufbau neuer TCP-Verbindungen genutzt werden.

Wenn der Mix feststellt, daß die TCP-Verbindung von der Gegenstelle geschlossen wurde, teilt er dies mit, indem er über die anonyme Verbindung ein RApplClosed-Paket sendet.

4.3.5.10 Data

In diesen Paketen leiten Mixe die verschlüsselten Daten der anonymen Verbindungen weiter. Ein Data-Paket besteht aus den eigentlichen Nutzdaten in den ersten 128 Bytes sowie aus sieben mal 16 Bytes, in denen jeweils das Typ-Byte und der MAC für die folgenden Mixe oder aber zufälliges Padding enthalten sind.

Der Mix entschlüsselt das Data-Paket und sendet dem folgenden Mix ein Paket, dessen Typ-Byte und MAC den Bytes 224–239 des entschlüsselten Pakets entnommen sind. Die übrigen aus Typ-Byte und MAC bestehenden Blöcke werden im neuen Data-Paket um jeweils eine Position verschoben übernommen; die Bytes 128–143 werden nach dem vom Absender angegebenen Padding-Algorithmus aufgefüllt. Die Bytes 0–127 des neuen Pakets sind die entschlüsselten Bytes 0–127 des Data-Pakets.

4.3.5.11 RData

Der Rückkanal zum anonymen Nutzer wird durch RData-Pakete implementiert. Um ein Paket in ein RData-Paket zu transportieren, kopiert der Mix die in den Bytes 0–127 enthaltenen Nutzdaten; die Bytes 144–255 der Eingabe werden in Bytes 128–239 des RData-Pakets übernommen. Der Mix berechnet dann den MAC des Pakets und verschlüsselt es mit dem vom anonymen Empfänger vorgegebenen Schlüssel. Da in RData-Paketen die Steuerinformationen – abgesehen von den MACs, deren Verfälschung automatisch dazu führt, daß das Paket als ungültig erkannt wird – im Gegensatz zu Data-Paketen keine Bedeutung tragen, wird der MAC bei diesen Paketen nur über die Bytes 0–127 gebildet.

Der lokale Mix des Nutzers entschlüsselt das empfangene RData-Paket nacheinander mit allen für die anonyme Verbindung vereinbarten symmetrischen Schlüsseln und prüft anhand der MACs seine Integrität. Wenn er einen Fehler feststellt, darf er nicht sofort alle anonymen Verbindungen unterbrechen, da ein aktiver Angreifer dann erkennen würde, zu welchem Nutzer die von ihm gestörte anonyme Verbindung gehört. Stattdessen erzeugt er in der folgenden Runde ein Data-Paket, das bei dem Mix, dessen MAC fehlerhaft war, und bei allen in der Sequenz folgenden Mixen zu einem Fehler führt und damit den Abbruch der Verbindung veranlaßt, ohne daß die Identität des Nutzers erkennbar wird.

4.3.5.12 Userdata, RUserdata

In Paketen dieses Typs werden die Nutzdaten durch die anonyme Verbindung übertragen. Der Inhalt eines Userdata-Pakets wird an eine vorher mit `AppleConnect` aufgebaute TCP-Verbindung gesendet. Daten, die ein Mix über eine solche TCP-Verbindung empfängt, leitet er in RUserdata-Paketen über die anonyme Verbindung weiter.

4.3.5.13 Close, Closed

Close-Pakete weisen den empfangenden Mix an, die jeweilige Verbindung zu schließen. Der Mix sendet daraufhin ein Closed-Paket an den Mix, von dem er das Close-Paket über die anonyme Verbindung erhalten hat; in der folgenden Runde geben beide Mixe den Kanal frei. Dieser wird dann mit Padding-Paketen aufgefüllt, bis er für eine neue Verbindung benötigt wird.

4.3.6 Verbindung zum Anwender

Der Mix des Nutzers akzeptiert auf einem dafür vorgesehenen Port Verbindungen von lokalen Proxies. Die Kommunikation zwischen Proxy und Mix erfolgt – analog zu Protokollen wie HTTP – zeilenweise; jede Zeile wird mit <CR><LF> beendet.

Durch diese Aufteilung zwischen Mix und Proxies, die im Klartext miteinander kommunizieren, können mit geringem Aufwand zusätzliche Proxies für weitere Protokolle entwickelt werden. Der Proxy benötigt keine kryptographischen Operationen und hat dennoch die vollständige Kontrolle über den Aufbau der anonymen Verbindung.

Beim Aufbau einer Verbindung meldet sich der Mix zunächst mit einer Statuszeile und der Liste der benachbarten Mixe. Wenn der Mix Verbindungen zu einer Anwendung aufbauen kann, enthält die Liste zusätzlich den Text `Application Proxy`. Sie endet mit dem Schlüsselwort `ok`.

Daraufhin kann der Proxy Kommandos senden. Der Mix antwortet darauf mit dem Inhalt der von ihm empfangenen und entschlüsselten Daten. Der Mix leitet den Inhalt von `RUserData`-, `CreateAck`- und `Error`-Paketen weiter. Die erste Zeile besteht aus dem Pakettyp gefolgt von der Länge der Nutzdaten in Bytes; in den folgenden Zeilen wird der Inhalt des Pakets wiedergegeben. Antworten, in denen keine Nutzdaten übermittelt werden, enthalten nur den Typ gefolgt von einem Punkt. Dies ist bei leeren `RUserData`-Paketen und bei `RAppClosed`-Paketen der Fall. `Padding`-Pakete werden nicht weitergeleitet.

Folgende Kommandos sind definiert:

4.3.6.1 NODE

Dem Schlüsselwort `NODE` folgt ein Leerzeichen und darauf der Name des Mixes, zu dem eine anonyme Verbindung aufgebaut werden soll. Falls der Name nicht gültig ist, gibt der Mix eine Fehlermeldung zurück. Andernfalls erzeugt er ein `Create`-Paket, um eine anonyme Verbindung aufzubauen, und sendet sie an den Nachbarn. Bei einem erfolgreichen Verbindungsaufbau beantwortet der benachbarte Mix die Verbindungsaufbau-nachricht mit einem `CreateAck`-Paket. Der in diesem Paket enthaltene

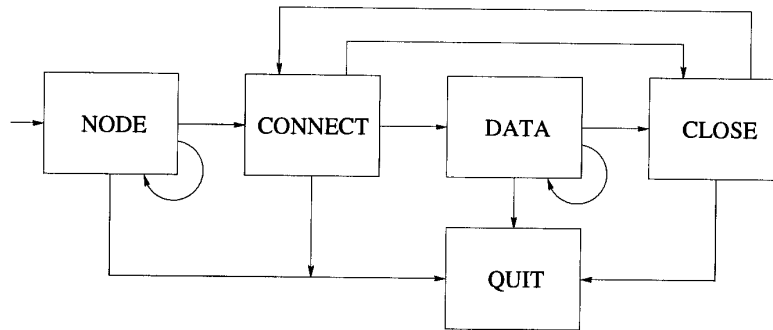


Abbildung 4.3: Abfolge der Kommandos

Text wird nach der Statuszeile an den Proxy übermittelt. Der Inhalt eines CreateAck-Pakets besteht entsprechend zum Verbindungsaufbau zum lokalen Mix aus einer Statuszeile und eine Liste der benachbarten Mixe. Statt der Bestätigung durch CreateAck kann der Proxy auch eine Fehlermeldung des Mixes in einem Error-Paket erhalten.

Weitere Kommandos, die der Proxy nach diesem Verbindungsaufbau sendet, werden anonymisiert an den ausgewählten Mix weitergeleitet. Sendet der Proxy ein NODE-Kommando, wenn schon eine anonyme Verbindung zu einem Mix besteht, dann wird diesem Mix zunächst ein Connect-Paket und darauf ein Create-Paket gesendet, so daß der Pfad der anonymen Verbindung um einen Mix verlängert wird. Das im CreateAck- oder Error-Paket enthaltene Ergebnis wird dem Proxy ausgegeben.

Bei einer bereits bestehenden längeren anonymen Verbindung werden das Connect- und das Create-Paket entsprechend der anonymen Verbindung verschlüsselt und in Data-Pakete eingepackt. Die in RData-Paketen verschlüsselt eintreffenden Antworten werden entschlüsselt und dann an den Proxy übermittelt.

4.3.6.2 CONNECT

Nachdem mit NODE-Kommandos eine anonyme Verbindung aufgebaut wurde, kann diese mittels CONNECT mit einem Empfänger verbunden werden. Der Mix erzeugt hierzu ein App1Connect-Paket, das durch die anonyme Verbindung gesendet wird. Dem CONNECT-Kommando kann ein Argument folgen; wenn keines angegeben ist, verwendet der empfangende Mix seinen vorgegebenen HTTP-Proxy.

4.3.6.3 DATA

DATA-Kommandos sind nur zulässig, wenn eine Verbindung zu einem Empfänger besteht. Der dem Schlüsselwort DATA und einem Leerzeichen fol-

```
WMIX daphne:5551
Node: amadeus:5552
ok
NODE amadeus:5552
CreateAck: 66
WMIX amadeus:5552
Node: daphne:5551
Application Proxy
ok
CONNECT
RUserdata.
RUserdata.
RUserdata.
DATA GET /
RUserdata.
RUserdata: 26
<HTML>Beispieltext</HTML>
RApplClosed.
QUIT
```

Abbildung 4.4: Dialog zwischen Proxy und lokalem Mix (gekürzt)

gende Text wird verschlüsselt in `Userdata`-Paketen über die anonyme Verbindung gesendet und vom letzten Mix an den Empfänger weitergeleitet. Die Zeile kann beliebig lang sein; um mehrzeilige Daten zu senden, müssen jedoch mehrere `DATA`-Kommandos gesendet werden.

Antworten des Empfängers treffen über die anonyme Verbindung in `RUserdata`-Paketen ein. Diese werden vom Mix entschlüsselt und an den Proxy weitergeleitet.

4.3.6.4 CLOSE

Durch ein `CLOSE`-Kommando wird der letzte Mix angewiesen, die Verbindung zur Anwendung zu schließen. Der Pfad durch das Mix-Netz bleibt jedoch bestehen und kann nach einem erneuten `CONNECT`-Kommando für weitere Datenübertragungen genutzt werden.

4.3.6.5 QUIT

Die Verbindung zwischen Mix und Proxy geschlossen. Anschließend wird die anonyme Verbindung abgebaut; zum Schutz gegen Verkehrsanalyse kann dies verzögert erfolgen.

4.4 Aufbau der Mix-Implementation WMix

Nach einer Initialisierungsphase durchläuft WMix eine Endlosschleife, in der Eingaben gelesen, verarbeitet und Ausgaben gesendet werden.

In der Initialisierungsphase liest WMix eine Konfigurationsdatei, initialisiert den Pseudozufallszahlengenerator (Abschnitt 4.5.2) und die Sockets und erzeugt bei Bedarf einen RSA-Schlüssel.

In der Eingabephase öffnet der Mix TCP-Verbindungen zu benachbarten Mixen und akzeptiert Verbindungen von Nachbarn sowie Client-Proxies. Außerdem liest er so lange Eingaben von den Sockets, bis er von allen aktiven Nachbarn alle für die jeweilige Runde vorgesehenen Pakete vollständig erhalten hat.

Daraufhin werden die empfangenen Pakete entschlüsselt und weitere durch den Pakettyp bestimmte Aktionen durchgeführt. Hierdurch werden die Ausgabepakete erzeugt; ungenutzte Pakete behalten ihren Initialisierungswert und sind daher padding-Pakete. Die Pakete werden im folgenden Schritt mit den jeweiligen Verbindungsschlüsseln verschlüsselt und an die benachbarten Mixe gesendet; in dieser Phase erfolgt auch die Ausgabe an Client-Proxies.

Die benachbarten Mixe speichert jeder Mix in einer Liste von Elementen des Typs `Node`, in der Adresse, Schlüssel, Zustandsinformationen und eine Liste der dem jeweiligen Mix zugeordneten Kanäle gespeichert sind. Für Client-Proxies dient eine Liste von Elementen des Typs `Proxy`, für ausgehende Verbindungen zu Servern eine Liste von Elementen des Typs `Out`.

Zur Verwaltung der Kanäle dient der Datentyp `Channel`. Ein `Channel` enthält Zustandsinformationen, Schlüssel für symmetrische Verschlüsselung, MACs und Padding und Verweise auf den in der anonymen Verbindung vorangehenden und nachfolgenden Kanal. Zusätzlich enthält er Speicherbereiche, in denen empfangende und zu sendende Pakete gespeichert werden.

Der Datenübertragung dient die Klasse `Socket`. Sockets können mit der Member-Funktion `connect`, die einen Hostnamen oder eine IP-Nummer sowie die Portnummer als Argument erhält, mit einem entfernten System verbunden werden oder mit `listen` und `accept` Verbindungen von anderen Systemen akzeptieren. Wenn ein `Socket` verbunden ist, können mit den üblichen Operatoren `<<` und `>>` sowie mit speziellen Funktionen Daten gelesen und geschrieben werden.

Die kryptographischen Operationen sind durch die Klassen `Cipher` (symmetrische Verschlüsselung), `PKCipher` (asymmetrische Verschlüsselung), `MAC` (Message Authentication Code) und `PAD` (Padding-Generator) implementiert. Member-Funktionen dieser Klassen rufen abhängig von der Auswahl des Algorithmus die OpenSSL-Funktionen auf, in denen die jeweiligen kryptographischen Algorithmen implementiert sind.

4.5 Die Verschlüsselungsbibliothek OpenSSL

OpenSSL [Young 1999] ist eine Bibliothek, die aus Implementationen kryptographischer Algorithmen und des SSL-Protokolls besteht. Sie war bis 1998 unter dem Namen SSLeay erhältlich.

OpenSSL ist in C programmiert und enthält Assembler-Implementationen der zeitkritischen Funktionen. Die Bibliothek kann unter Unix und Windows eingesetzt werden und darf nichtkommerziell wie auch kommerziell frei verwendet werden. Da die Bibliothek im Quellcode zur Verfügung steht, kann sie an die Bedürfnisse des Benutzers individuell angepaßt werden. Der in OpenSSL 0.9.1c noch nicht enthaltene neue OAEP-Modus für die RSA-Verschlüsselung konnte so zur Bibliothek hinzugefügt werden.

OpenSSL unterstützt die Algorithmen RSA, DSA, Diffie-Hellman, Blowfish, CAST, DES, IDEA, MDC2, RC2, RC4, RC5, MD2, MD5, RIPEMD-160, SHA-1 und HMAC [Schneier 1996]. Es stehen Funktionen zum Erzeugen von Pseudozufallszahlen und zum Umgang mit beliebig großen Zahlen zur Verfügung.

4.5.1 OAEP

In OpenSSL 0.9.1c wird RSA-Verschlüsselung nach PKCS #1 Version 1.5 sowie eine für SSL verwendete Variante unterstützt. Der in PKCS #1 Version 2.0 [Kaliski 1998] neu eingeführte OAEP-Modus wurde für die Verwendung in WMix neu implementiert.

Zum Erzeugen bzw. Prüfen der OAEP-Kodierung dienen die neuen Funktionen `RSA_padding_add_PKCS1_OAEP()` und `RSA_padding_check_PKCS1_OAEP()`. Diese Funktionen haben dieselben Parameter wie ihre PKCS1v1_5-Entsprechungen sowie zusätzlich den OAEP-Kodierungsparameter, der in [Kaliski 1998] vorgesehen ist, um für verschiedene Zwecke erzeugte Geheimtexte voneinander unterscheiden zu können, der aber im Normalfall die Länge 0 hat.

Diese Funktionen werden von den üblichen RSA-Funktionen `RSA_public_encrypt()` und `RSA_private_decrypt()` aufgerufen, wenn der Parameter `padding` den Wert `RSA_PKCS1_OAEP_PADDING` hat.

Zur Verwendung in der OAEP-Verschlüsselung definiert [Kaliski 1998] die Maskengenerierungsfunktion MGF1, die als Eingabe eine Zeichenkette und die Angabe einer gewünschten Ausgabelänge erhält und eine durch die Eingabe determinierte pseudozufällige Zeichenkette der gewünschten Länge ausgibt. MGF1 verwendet dazu eine Hashfunktion; in der vorliegenden Implementation ist hierfür SHA-1 vorgesehen.

4.5.2 Der Zufallszahlengenerator

Die Erzeugung von Zufallszahlen ist für die Sicherheit kryptographischer Systeme von entscheidender Bedeutung. Dies betrifft beispielsweise die

Erzeugung der Schlüsselpaare und der symmetrischen Sitzungsschlüssel. Wenn ein Angreifer die hierfür verwendeten Zufallszahlen errät, kann er die jeweiligen Daten entschlüsseln.

Die unmittelbare Erzeugung zufälliger Daten wird von derzeit üblicher PC-Hardware nicht unterstützt. Daher müssen per Software Pseudozufallszahlen erzeugt werden, die durch Angreifer nicht zu erraten sind. Dafür benötigt ein *Pseudozufallszahlengenerator (PRNG)* einen zufälligen Initialisierungswert, der so groß ist, daß die möglichen Initialisierungswerte nicht systematisch ausprobiert werden können. Auch muß verhindert werden, daß aus einer Folge von Pseudozufallszahlen auf vorhergehende oder nachfolgende Zahlen geschlossen werden kann.

Zur Erzeugung eines Initialisierungswertes kann auf die Hardware zurückgegriffen werden [Eastlake 1994]. Beispielsweise können physikalische Effekte in Festplatten als Quelle von Zufallszahlen genutzt werden. Auch die Bewegung des Mauszeigers oder die Eingabe zufälliger Tastendrucke durch den Nutzer ist für einen Angreifer nicht nachvollziehbar und kann daher für den Zufallszahlengenerator genutzt werden.

Viele neuere Unix-artige Betriebssysteme unterstützen die Erzeugung von Zufallszahlen, indem sie die Zeitpunkte von Hardware-Interrupts, Maus-Koordinaten und vergleichbare Angreifern nicht bekannte Daten verwenden. Wenn er vorhanden ist, nutzt OpenSSL diesen Zufallszahlengenerator; andernfalls muß die jeweilige Anwendung den PRNG von OpenSSL vor der Benutzung initialisieren. Hierfür stehen Funktionen zur Verfügung, mit denen der Zustand des PRNG in einer Datei gespeichert und wieder geladen werden kann, so daß nur vor der ersten Benutzung ein zufälliger Initialisierungswert erzeugt werden muß.

Kapitel 5

Performanz

Die Performanz ist für die Benutzerfreundlichkeit eines Anonymisierungsverfahrens von entscheidender Bedeutung, da ein Verfahren mit zu großer Verzögerung von den Anwendern nicht akzeptiert werden würde. Zudem spielt das Zeitverhalten des Netzes auch für die Sicherheit eine Rolle, da auf dem Zeitverhalten beruhende Angriffe möglich sind. Daher wurde die im vorhergehenden Kapitel beschriebene Implementation in einem praktischen Versuch erprobt.

5.1 Auswirkungen für den Anwender

Bei der Benutzung eines interaktiven Dienstes erwartet der Nutzer, daß seine Anfragen möglichst schnell beantwortet werden. Zu betrachten ist zum einen die *Verzögerung*, d. h. der Zeitraum zwischen dem Absenden der Anfrage und dem Beginn des Empfangens der Antwort und zum anderen der *Durchsatz*, also die Anzahl der übertragenen Bytes pro Sekunde.

5.1.1 Verzögerung

Eine Verzögerung ergibt sich dadurch, daß das Mix-Verfahren in Runden durchgeführt wird. Daten können also nicht sofort übertragen werden, sondern der Sender muß warten, bis ein hierfür zur Verfügung stehender Kanal an der Reihe ist. Jeder an der Übertragung beteiligte Mix empfängt sämtliche Pakete der jeweiligen Runde, bevor er sie entschlüsselt und in der folgenden Runde weiterleitet (Abschnitt 4.3.4). Die Verzögerung hängt somit von der Anzahl der verwendeten Mixe und für jeden einzelnen Mix von der Anzahl der verwendeten Kanäle ab.

Neben dieser durch das Weiterleiten der Daten durch das Mix-Netz bedingten Verzögerung verursacht die Anonymisierung auch eine Begrenzung des Datendurchsatzes.

5.1.2 Durchsatz

Da ein Mix empfangene Daten erst dann weiterleiten kann, wenn er alle zur jeweiligen Runde gehörenden Pakete empfangen hat, ist der Durchsatz des Mix-Netzes durch den Durchsatz der langsamsten Verbindung zwischen zwei Mixen begrenzt. Zudem werden zwischen je zwei Mixen in jeder Runde mehrere Pakete übertragen, so daß die zur Verfügung stehende Bandbreite auf die bestehenden Kanäle aufgeteilt werden muß. Da die Anzahl der bestehenden anonymen Verbindungen für externe Angreifer nicht erkennbar sein soll, müssen immer auch ungenutzte Kanäle bestehen, in denen nur Padding übertragen wird.

Verzögerungen, die auf zusätzlichem Verkehr im dem Anonymisierungsverfahren zugrundeliegenden Datennetz oder auf anderweitiger Auslastung der Rechner beruhen, wirken sich auf alle anonymen Verbindungen aus.

Neben der Geschwindigkeit der Datenübertragung spielen auch die kryptographischen Operationen eine Rolle. Die Durchführung des RSA-Algorithmus ist aufwendig; sie tritt nur beim Verbindungsaufbau auf. Der Nutzer muß zudem alle gesendeten Pakete für alle von ihm ausgewählten Mixe nacheinander mit einem symmetrischen Algorithmus ver- und die empfangenen Pakete entschlüsseln. Jeder Mix führt für jedes weitergeleitete Paket eine symmetrische Verschlüsselungsoperation durch.

5.2 Praktische Erprobung

5.2.1 Durchführung

Zur Erprobung der Performanz wurden Mix-Netze in verschiedenen Konstellationen aufgebaut. Die Mix-Software wurde um die Möglichkeit ergänzt, die Typen der übertragenen Pakete mit Zeitstempeln versehen zu protokollieren. Zur Auswertung der Protokolldateien wurden Perl-Skripte eingesetzt.

Verwendet wurde zum einen ein Netz aus Windows 98-Systemen, zum anderen ein Unix-Netz, in beiden Fällen auf Ethernet-Basis. Die Funktion `GetSystemTime()` liefert die Zeit unter Windows 98 mit einer Auflösung von mehreren Hundertstelsekunden. Bei dieser Genauigkeit sind Auswertungen zwar möglich, eine höhere Auflösung ist jedoch wünschenswert. Im Sparc-basierten Unix-Netz können die Zeiten mit einer Genauigkeit einer Tausendstelsekunde gemessen werden.

Es wurden Mix-Netze verschiedener Größe eingesetzt und Pfade verschiedener Länge durch das Mix-Netz verwendet. Während eines Teils der Versuche wurde zusätzlicher Verkehr auf dem Ethernet erzeugt, indem parallel ein zweites Mix-Netz zum Einsatz gebracht wurde.

Um die Auswirkung der RSA-Verschlüsselung feststellen zu können, wurde eine zusätzliche Messung durchgeführt, bei der die asymmetrische

Konfiguration (Win98-Netz)	Minimum	Maximum	Durchschnitt	bei Create
2 Mixe	60	770	323	440
4 Mixe	0	2200	407	660
2 Mixe, 2. Mix-Netz parallel	0	1430	423	270
2 Mixe, kein RSA	60	710	387	440

Konfiguration (Unix-Netz)	Minimum	Maximum	Durchschnitt	bei Create
2 Mixe	94,7	191,8	101,7	112,3
4 Mixe	89,9	190,1	101,0	113,3
2 Mixe, 2. Mix-Netz parallel	87,7	180,0	99,0	101,5
2 Mixe, kein RSA	90,7	160,3	90,7	114,5
4 Mixe, kein RSA	96,2	140,2	100,7	108,6

Abbildung 5.1: Dauer einer Mix-Runde in 1/1000 Sekunden

Verschlüsselung ausgelassen wurde. Bei der Messung ergaben sich die in Tabelle 5.1 wiedergegebenen Zeiten.

Die symmetrische Verschlüsselung spielt eine geringere Rolle, da symmetrische Algorithmen schneller ablaufen. Zudem sind sie für die Verkehrsanalyse weniger wichtig, da ein Mix in jeder Runde annähernd gleichviele symmetrische Verschlüsselungsoperationen durchführt.

Im Testnetz mit zwei Mixen wurden Dateien verschiedener Größe übertragen. Die Übertragung einer 6 kB großen Datei durch das Mix-Netz dauerte 2,55 Sekunden. Für eine 50 kB große Datei waren 37 Sekunden erforderlich. Die Übertragung einer Datei, in der 10 *inline*-Grafiken angefordert wurden, dauerte 55 Sekunden. Hierbei ist durch eine andere Arbeitsweise der HTTP-Proxies eine deutliche Beschleunigung möglich. Die im Rahmen dieser Arbeit verwendeten Proxies leiten Nachrichten erst weiter, nachdem sie sie vollständig empfangen haben. Werden alle empfangenen Daten sofort weitergeleitet, ergibt sich insbesondere in Fällen, in denen große Dateien übertragen werden, eine geringere Verzögerung. Zu berücksichtigen ist auch, daß das Erzeugen der Protokolldatei selbst ebenfalls Zeit kostet. Im realen Einsatz sind daher höhere Geschwindigkeiten möglich, als sie bei der Messung festgestellt werden.

5.2.2 Auswertung

Bei der Dauer der Runden zeigen besonders im Windows-Netz sich deutliche Schwankungen. Im Fall von Create-Paketen ist die Verzögerung überdurchschnittlich groß; sie liegt jedoch in jedem Fall unterhalb der maximalen im Mix-Netz aufgetretenen aufgetretenen Verzögerungszeit. Es ergibt sich, daß die Verzögerung durch die RSA-Entschlüsselung auf den verwendeten Pentium-PCs akzeptabel ist. Im Unix-Netz zeigten sich geringere Schwankungen, aber auch in diesem Fall liegt die Verzögerung durch Verbindungsaufbaunachrichten unterhalb der maximal aufgetretenen Verzö-

gerungszeit. Es ist demnach nicht erforderlich, die Entschlüsselung in einem separaten Thread durchzuführen.

Beim Einsatz eines Mix-Netzes im lokalen Netz war der Datendurchsatz im Vergleich zur nicht anonymisierten Form deutlich reduziert. Er lag jedoch in dem Bereich, der bei Modem-Übertragung üblich ist. Für ein verteiltes Mix ist eine vergleichbare Performanz möglich, wenn Mix-Netz-Verbindungen nur zwischen Systemen hergestellt werden, zwischen denen eine schnelle Internet-Verbindung besteht.

5.2.3 Ergebnis

Das WMix-Verfahren verursacht eine deutliche, aber in der Regel akzeptable Verzögerung beim Zugriff auf WWW-Seiten. Kryptographische Operationen sind anhand der Übertragungszeit nicht zu identifizieren, so daß zusätzliche absichtliche Verzögerungen zur Abwehr von Angriffen durch Verkehrsanalyse nicht erforderlich sind.

Kapitel 6

Sicherheit

Ein Mix-Netz ist sicher, wenn weder passive noch aktive Angreifer Informationen über die Nutzer gewinnen können. Vorausgesetzt ist in jedem Fall, daß ein Teil der Nutzer und mindestens einer der Mixe vertrauenswürdig ist (Abschnitt 3.2).

6.1 Verkehrsanalyse

Ein passiver Angreifer, der ein Mix-Netz beobachtet, kann gewisse Informationen über die Benutzung des Netzes erhalten. Zu untersuchen ist, welche Informationen der Angreifer bei der WMix-Implementation aus den übertragenen Daten gewinnen kann, und welche Informationen das Zeitverhalten des Mix-Netzes ihm gibt.

6.1.1 Externer Angreifer

Für Nutzer, die keine permanente Internet-Verbindung haben, ist in jedem Fall dadurch ein statistischer Angriff möglich, daß eine Korrelation zwischen den Zeitpunkten anonymer Verbindungen zu bestimmten Systemen und den Verbindungen eines Nutzers zum Mix-Netz festgestellt werden können (vgl. Abschnitt 3.4.3). Dieser Angriff läßt sich nur um den Preis

Angreifer	passiv	aktiv
extern	wirkungslos	denial of service
intern	Analyse des Verbindungsaufbaus	Verfälschung in der Rückrichtung

Abbildung 6.1: Mögliche Angriffe gegen das Mix-Netz

permanenter Datenübertragung verhindern; solange Internet-Zugriffe vorwiegend über Telefon-Einwahl erfolgen, ist er also nicht vermeidbar.

Wenn konkrete Datenübertragungen eines Nutzers beobachtet werden können, ist dieser Angriff nicht mit hohem Aufwand verbunden. Weniger Informationen stehen dem Angreifer zur Verfügung, wenn die Software des Nutzers während der Dauer der Verbindung in festen Abständen Daten sendet und empfängt, die tatsächlichen Sendevorgänge also durch Padding verdeckt werden. Dies ist bei WMix der Fall, da auf dem System des Nutzers ein eigener Mix mit Padding auf den Kommunikationsverbindungen läuft.

Nachdem eine Verbindung zwischen zwei Mixen aufgebaut wurde, findet dort die gesamte Datenübertragung verschlüsselt statt. Nur das `SessionKey`-Paket und das gleichzeitig vom anderen Mix gesendete `Padding`-Paket zu Beginn der Verbindung sind nicht symmetrisch verschlüsselt; für einen Angriff nützliche Daten sind ihnen jedoch nicht zu entnehmen. In Verbindung mit dem Padding auf der Verbindung führt dies dazu, daß passive externe Angriffe wirkungslos sind.

6.1.2 Interner Angreifer

Einem internen Angreifer bieten sich weitere Möglichkeiten der Verkehrsanalyse, da er den Typ und Inhalt der Pakete kennt, die die von ihm kontrollierten Mixe empfangen. Der Angreifer kann also den Verbindungsauf- und -abbau mittels `Create`- und `Close`-Paketen beobachten; wenn dieser in zeitlichem Zusammenhang mit einem anonymen Zugriff auf einen WWW-Server steht, tragen die in der Mix-Sequenz auf den Angreifer folgenden Systeme nicht zur Sicherheit bei. WMix ermöglicht es, eine Verbindung schrittweise auf- und abzubauen. Die in einer Verbindung verwendeten Mixe empfangen die jeweiligen `Create`-Pakete also nicht unmittelbar nacheinander; vielmehr der Zeitraum beliebig ausgedehnt werden, wenn der jeweils verwendete Client-Proxy diese Funktion unterstützt. Dadurch kann der Angreifer von den beobachteten Paketen nicht mehr auf tatsächliche anonyme Verbindungen schließen. Die Nutzdaten liegen bei allen Mixen mit Ausnahme des ersten und des letzten nur in verschlüsselter Form vor. Der erste Mix steht unter der Kontrolle des Nutzers. Der letzte kennt den Server, mit dem anonym kommuniziert wird und die übertragenen Daten. Wenn der Pfad einen Mix enthält, der nicht mit dem Angreifer kooperiert, ist der Nutzer jedoch auch gegenüber den nachfolgenden Mixen anonym.

6.2 Zeitverhalten

Eine Gefahr für die Vertraulichkeit besteht, wenn Angreifer aus Verzögerungen bei der Datenübertragung Rückschlüsse auf übertragene Inhalte

ziehen kann. Diese Gefahr besteht besonders bei Verzögerungen, die durch die zeitaufwendigen asymmetrischen Verschlüsselungsoperationen entstehen.

6.2.1 Kryptographische Operationen

Für verschiedene Eingaben laufen kryptographische Operationen unterschiedlich schnell ab. Ein Angreifer, der den Inhaber eines geheimen Schlüssels dazu bringt, bestimmte Daten zu entschlüsseln, und die Zeit der Entschlüsselungsoperation mißt, kann dadurch auf den geheimen Schlüssel schließen [Kocher 1996]. Da Mixe automatisch Daten entschlüsseln, müssen Maßnahmen gegen diesen Angriff getroffen werden. Ein möglicher Schutz besteht bei RSA darin, den Geheimtext vor der Entschlüsselung durch Multiplikation mit einer Zufallszahl zu *blenden*. Diese Möglichkeit wird von OpenSSL unterstützt.

Einem externen Angreifer kann schon die Tatsache, daß ein Mix überhaupt eine RSA-Entschlüsselung durchführt, Informationen darüber geben, auf welchem Pfad eine anonyme Verbindung aufgebaut wird (Abschnitt 4.3.5.4). Wenn eine Entschlüsselung länger dauern würde als eine Runde des Mix-Protokolls, müßte der Mix daher ohne Unterbrechung weiter Daten übertragen, während er Verbindungsaufbaunachrichten entschlüsselt.

6.2.2 Verzögerung durch andere Prozesse

Keine Angriffspunkte entstehen, wenn die Datenübertragung eines Mixes dadurch verzögert wird, daß er auf Daten von einem benachbarten Mix warten muß, oder daß ein anderer Prozeß mit höherer Priorität als der Mix bearbeitet wird. Ausgenommen davon sind Verzögerungen auf dem Computer des Nutzers selbst, die durch die anonym abgerufenen Inhalte bedingt sind. Problematisch sind in der Hinsicht vor allem aktive Inhalte wie Applets, die aus Sicherheitsgründen deaktiviert werden sollten. Unter Umständen kann ein Angreifer jedoch schon aus der für das Darstellen einer HTML-Seite benötigten Zeit Rückschlüsse auf den Inhalt ziehen. Ein solcher Angriff läßt sich nicht vollständig verhindern.

6.3 Nicht-anonyme Datenübertragung

Eine Sicherheitslücke besteht, wenn ein WWW-Browser Daten überträgt, ohne den Proxy zu verwenden. Der Nutzer muß daher für alle Protokolle, auch beispielsweise für ftp, einen anonymisierenden Proxy eintragen.

Wichtig ist auch, daß der verwendete Browser keine DNS-Anfragen bezüglich der Adressen durchführt, auf die anonym zugegriffen werden soll. Bei Zugriffen über einen Proxy sind DNS-Anfragen nicht erforderlich; eine

beliebte Funktion von Browsern besteht allerdings darin, unvollständige Hostnamen zu ergänzen, indem überprüft wird, ob der eingegebene Name mit den Ergänzungen `www` und `.com` oder `.net` existiert. *Netscape* und *Internet Explorer* führen diese Funktion bei Zugriffen über Proxy-Server nicht aus. Der Browser *Lynx* führt sie dagegen immer aus, wenn als Adresse kein vollständiger URL eingegeben wurde, auch wenn ein HTTP-Proxy eingetragen ist. Derartige Browser können nur eingesetzt werden, wenn alle DNS-Anfragen durch einen Firewall herausgefiltert werden.

6.4 Aktive Angriffe

Die im vorangehenden Abschnitt betrachteten Angriffe beruhen darauf, daß der Angreifer bestimmte Daten beobachtet und auswertet. Darüberhinaus ist zu berücksichtigen, daß ein Angreifer auch selbst in die Datenübertragung eingreifen kann, um Informationen zu erlangen.

6.4.1 Externer Angreifer

Wenn ein Angreifer eine bestehende Verbindung zwischen zwei Mixen stört, indem er Daten verfälscht, wird dies vom empfangenden Mix erkannt. Ein Mix, der ungültige Daten empfängt, oder feststellt, daß eine TCP-Verbindung geschlossen wurde, beendet sich. Daraufhin terminieren auch die benachbarten Mixe. Anonyme Kommunikation kann erst nach dem Neustart des Systems fortgesetzt werden. Dadurch sind *denial of service*-Angriffe möglich; die Anonymität der Nutzer ist aber nicht gefährdet.

Wenn der Angreifer bereits verhindert, daß zwischen zwei Mixen eine Verbindung aufgebaut wird, arbeiten die Mixe auf ihren anderen Verbindungen wie üblich. Daß Sicherheit durch ein kleineres zur Verfügung stehendes Mix-Netz reduziert ist, kann der Nutzer der Ausgabe seines Client-Proxies entnehmen und seine Nutzung daran anpassen.

Während des Verbindungsaufbaus zwischen zwei Mixen wird der symmetrische Sitzungsschlüssel mit dem öffentlichen Schlüssel des einen Mixes verschlüsselt; ein Angreifer könnte sich für den anderen Mix ausgeben, da dieser nicht kryptographisch authentifiziert wird. Der Angreifer könnte anonyme Daten jedoch nicht entschlüsseln, da sie in jedem Fall mit dem zertifizierten Schlüssel des echten Mixes verschlüsselt sind. Ein derartiger Angriff kann die Anonymität der Nutzer also nicht kompromittieren.

6.4.2 Interner Angreifer

Ein interner Angreifer kann seinen Nachbarn gültige Pakete senden. Auf bereits bestehenden anonymen Verbindungen wird der MAC jedoch vom Nutzer selbst erzeugt, so daß interne Angriffe dabei erkannt werden. In der

Rückrichtung ist die Prüfung des MAC nur durch den lokalen Mix des Nutzers möglich. Wenn dieser einen Angriff feststellt, sendet er in der folgenden Runde ein Paket, das für den Mix, bei dem der Angriff stattfindet, und die darauf folgenden Mixe ungültige Daten enthält (*jamming*; Abschnitt 4.3.5.11). Diese Mixe können den Angriff daraufhin erkennen und terminieren. Der interne Angreifer kann dann nicht feststellen, zu welchem Nutzer die von ihm gestörte Verbindung gehört. Anhand die Verzögerung bis zum Abbruch des Mix-Verfahrens kann er allerdings erkennen, durch wieviele Mixe das *jamming*-Paket weitergeleitet wurde, wie lang also der Pfad durch das Mix-Netz ist.

Gegen Angriffe auf die Kommunikation zwischen dem Nutzer und seinem lokalen Mix ist bei WMix kein Schutz vorgesehen. Hier muß der Nutzer sicherstellen, daß sein lokales System bzw. lokales Netz sicher ist.

Kapitel 7

Zusammenfassung und Ausblick

Mix-Netz-basierte Anonymisierungsverfahren bieten eine praktikable Lösung für die im Internet bestehenden Datenschutzprobleme. Bei Zugriffen auf das WWW fällt eine Vielzahl personenbezogener Daten an. Dies kann vermieden werden, indem die Zugriffe in anonymisierter Form erfolgen.

Das 1981 von D. Chaum zum Schutz von E-Mail konzipierte Mix-Netz wurde seither weiterentwickelt; es wurden verschiedene Varianten vorgeschlagen, mit denen Daten interaktiv übertragen werden können. Am Beispiel von Zero Knowledge Systems, Inc. zeigt sich, daß auch Interesse an der kommerziellen Nutzung dieser Verfahren besteht. Die bestehenden Verfahren wie Onion Routing weisen allerdings noch einige Schwächen auf; auch stehen der Nutzung von Onion Routing außerhalb der USA die Exportbestimmungen für kryptographische Software entgegen.

In dieser Arbeit wurde gezeigt, welche Anforderungen ein Anonymisierungsverfahren für WWW-Zugriffe erfüllen muß. Im Anschluß an eine Untersuchung der bestehenden Systeme in Bezug auf diese Anforderungen wurde ein Mix-Netz-basiertes Protokoll vorgeschlagen und in C++ für Windows und Unix implementiert. Eine Untersuchung der gegen dieses Verfahren möglichen Angriffe und eine praktische Erprobung zeigen, daß der Datenschutz hiermit gewährleistet werden kann. Es besteht jedoch ein Konflikt zwischen der Sicherheit und der Verfügbarkeit, da viele aktive Angriffe nur verhindert werden können, indem das gesamte Mix-Netz angehalten und neu gestartet wird. Hier muß für die einzelne Anwendung entschieden werden, ob *denial of service*-Angriffe hingenommen werden können, um einen zuverlässigen Schutz der Anonymität zu gewährleisten.

7.1 Mögliche Weiterentwicklungen

Die in dieser Arbeit entwickelte Software kann durch Anpassungen des Mix-Netzes an das Nutzerverhalten und durch Verbesserungen der Benut-

zerschnittstelle weiterentwickelt werden.

7.1.1 Verbesserung der Benutzerschnittstelle

WMix und AFproxy sind Textmodus-Programme, die Informationen über ihren Zustand zeilenweise ausgeben. Sie sind dadurch für Tests gut geeignet; um jedoch für die praktische Anwendung eine höhere Benutzerfreundlichkeit zu erreichen, sollte die von Anwendern installierte Software vollständig mit einer graphischen Oberfläche ausgestattet sein. Hierfür kann der WWW-Browser des Nutzers eingesetzt werden. Die Konfiguration kann dabei durch vom Proxy erzeugte HTML-Formulare vorgenommen werden. Rückmeldungen über den Zustand der anonymen Verbindung können in einem zusätzlichen Fenster des Browsers angezeigt werden.

7.1.2 Anpassungen des Mix-Protokolls

Es ist denkbar, daß Anpassungen des Protokolls an das Nutzerverhalten nötig werden. Wenn ein Mix-Netz viele Nutzer hat oder einige Nutzer die Datenübertragung absichtlich stören, sind häufige Übertragungsabbrüche zu erwarten. Die Robustheit des Mix-Netzes kann erhöht werden, wenn eine reduzierte Sicherheit akzeptabel ist. Um aktive Angriffe auf die Anonymität eines Nutzers zu verhindern, bricht WMix die gesamte Kommunikation ab, sobald die Integrität der Übertragung gestört ist (siehe Abschnitt 3.4.2). Wenn der maximal mögliche Schutz gegen aktive Angreifer nicht erforderlich ist, kann stattdessen nur die betroffene anonyme Verbindung geschlossen werden. Die Auswirkung eines *denial of service*-Angriffs ist dann auf die betroffene Verbindung beschränkt.

Auch Änderungen bei den eingesetzten Algorithmen sind möglich, wenn sich beispielsweise herausstellt, daß bestimmte in WMix verwendete kryptographische Algorithmen unsicher sind, oder wenn Algorithmen entwickelt werden, die bei vergleichbarer Sicherheit schneller sind als die in WMix eingesetzten. Dies ist problemlos möglich, da die jeweils verwendeten Algorithmen beim Schlüsselaustausch bzw. beim Verbindungsaufbau spezifiziert werden. Damit sind auch Anpassungen an Weiterentwicklungen in der Kryptologie möglich.

7.2 Vorschlag einer praktischen Mix-Architektur

Um Nutzern im Internet die Nutzung eines Mix-Netzes zu ermöglichen, muß die nötige Software und ein Verzeichnis der öffentlichen Schlüssel bereitgestellt werden. Hierfür sollte die Mix-Software WMix als Windows-Version und für Unix-artige Betriebssysteme im Quellcode auf einem ftp- oder WWW-Server zur Verfügung gestellt werden. Dieser Server sollte zusätzlich eine regelmäßig aktualisierte Liste der gegenwärtig aktiven Mixe

und ihrer öffentlichen Schlüssel enthalten. Nützlich wären auch Informationen für neue Benutzer, in denen der Zweck und die Installation der Software dargestellt wird. Zudem sollte auf diesem System ein Mix betrieben werden, zu dem die Nutzer und weitere unabhängige Betreiber Verbindungen aufbauen können.

Um anonym auf das WWW zugreifen zu können, installiert der Nutzer die Software sowie die aktuelle Liste auf seinem Computer; er kann die Konfiguration an seine Sicherheitsanforderungen anpassen, indem er eine Pfadlänge für die zufällige Auswahl von Mixen wählt und Mixe aus der Liste entfernt, denen er nicht vertraut. Nachdem der Mix-Client im WWW-Browser als Proxy eingetragen wurde, erfolgen die WWW-Zugriffe dann anonym.

Wer selbst einen Mix betreiben will, benötigt eine permanente Verbindung zum Internet. Er kann einen oder mehrere der bereits vorhandenen Mixe als Nachbarn wählen, wobei es sich anbietet, Mixe auszuwählen, zu denen eine schnelle Internet-Verbindung besteht. Nach der Installation der Software trägt der Betreiber sein System in die Liste der aktiven Mixe ein. Beim Programmstart erzeugt WMix dann ein RSA-Schlüsselpaar. Der Betreiber teilt dem Verwalter der Mix-Liste die Adresse und den öffentlichen Schlüssel seines Mixes mit. Sobald der neue Mix in die Liste aufgenommen wird, kann er von allen Nutzern in anonymen Verbindungen verwendet werden.

Literaturverzeichnis

- [Beaver 1992] D. Beaver: „Foundations of Secure Interactive Computing“. *Advances in Cryptology: Crypto '91*, Springer, 1992, S. 377–391.
- [Bellare 1995] M. Bellare, P. Rogaway: „Optimal Asymmetric Encryption – How to Encrypt with RSA“. *Advances in Cryptology: Eurocrypt '94*, Springer, 1995, S. 92–111.
- [Bellare 1997] M. Bellare, P. Rogaway: „Minimizing the Use of Random Oracles in Authenticated Encryption Schemes“. *Information and Communications Security, ICICS '97*, Springer, 1997.
- [Berners-Lee 1995] T. Berners-Lee, D. Connolly: „Hypertext Markup Language – 2.0“. *Internet RFC 1866*, November 1995.
- [Berners-Lee 1998] T. Berners-Lee, R. Fielding, L. Masinter: „Uniform Resource Identifiers (URI): General Syntax“. *Internet RFC 2396*, August 1998.
- [Bleichenbacher 1998] D. Bleichenbacher: „Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1“. *Advances in Cryptology - Crypto '98*, Springer, 1998, S. 1–12.
- [Callas 1998] J. Callas, L. Donnerhake, H. Finney, R. Thayer: „OpenPGP Message Format“. *Internet RFC 2440*, November 1998.
- [Chaum 1981] D. Chaum: „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms“. *Communications of the ACM* 24 (1981) 2, S. 84–88.
- [Chaum 1988] D. Chaum: „The Dining Cryptographers Problem. Unconditional Sender and Recipient Untraceability“. *Journal of Cryptology* 1 (1988) 1, S. 65–75.
- [Cottrell 1995] L. Cottrell: „Mixmaster and Remailer Attacks“, 1995. URL: <http://www.obscura.com/~loki/remailer/remailer-essay.html>

- [Dai 1998] W. Dai: „PipeNet 1.1“, 1998. URL: <http://www.eskimo.com/~weidai/pipenet.txt>
- [Demuth 1998] T. Demuth, A. Rieke: „Anonym im World Wide Web?“ *Datenschutz und Datensicherheit* 22 (1998) 11, S. 623–637.
- [Eastlake 1994] D. Eastlake, S. Crocker, J. Schiller: „Randomness Recommendations for Security“. *Internet RFC 1750*, Dezember 1994.
- [EFF 1998] Electronic Frontier Foundation: *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*, O'Reilly & Associates, 1998.
- [Fielding 1997] R. Fielding et al.: „Hypertext Transfer Protocol – HTTP/1.1“. *Internet RFC 2616*, Juni 1999.
- [FIPS 1980] US Department of Commerce/National Bureau of Standards: „Data Encryption Standard“. *Federal Information Processing Standards Publication 81*, 1980.
- [FIPS 1995] US Department of Commerce/N.I.S.T.: „Secure Hash Standard“. *Federal Information Processing Standards Publication 180-1*, 1995.
- [Franz 1997] E. Franz, A. Jerichow, A. Pfitzmann: „Systematisierung und Modellierung von Mixen“. *Verlässliche IT-Systeme, GI-Fachtagung VIS '97*, Vieweg, 1997, S. 172–190.
- [Freier 1996] A. Freier, P. Karlton, P. Kocher: „The SSL Protocol Version 3.0“, 4. März 1996. URL: <ftp://ftp.netscape.com/pub/review/ssl-spec.tar.z>
- [Goldberg 1997] I. Goldberg, D. Wagner: „TAZ Servers and the Reweaver Network – Enabling Anonymous Publishing on the World Wide Web“, CS 268 Final Project, University of California, Berkeley, 1997. URL: <http://http.cs.berkeley.edu/~daw/cs268/taz.ps>
- [Goldreich 1997] O. Goldreich: „The Foundations of Modern Cryptography“, Version 2.2, 1997. URL: <http://theory.lcs.mit.edu/~oded/tfoc.html>. Vorläufige Fassung in: *Crypto '97*, S. 46–74.
- [Goldwasser 1997] S. Goldwasser, M. Bellare: „Lecture Notes on Cryptography“, 19. Juni 1997. URL: <http://www-cse.ucsd.edu/~mihir/papers/gb.ps.gz>

- [Gülcü 1996] C. Gülcü, G. Tsudik: „Mixing Email with BABEL“. *1996 Symposium on Network and Distributed System Security*, IEEE Computer Society Press, 1996, S. 2–16.
- [Johns 1993] M. Johns: „Identification Protocol“. *Internet RFC 1413*, Februar 1993.
- [Kaliski 1998] B. Kaliski, J. Staddon: „PKCS #1: RSA Cryptography Specifications, Version 2.0“. *Internet RFC 2437*, Oktober 1998.
- [Kesdogan 1998] D. Kesdogan, J. Egner, R. Büschkes: „Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System“. *Information Hiding 1998*, Springer, 1998, S. 83–98.
- [Kocher 1996] P. Kocher: „Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems“. *Advances in Cryptology: Crypto '96*, Springer, 1996, S. 104–113.
- [Krawczyk 1997] H. Krawczyk, M. Bellare, R. Canetti: „HMAC: Keyed-Hashing for Message Authentication“. *Internet RFC 2104*, Februar 1997.
- [Kristol 1997] D. Kristol, L. Montulli: „HTTP State Management Mechanism“. *Internet RFC 2109*, Februar 1997.
- [Lahey 1999] A. Lahey: „What price privacy?“ *Canadian Business*, 26. Februar 1999.
- [Martin 1998] D. Martin: „A Framework for Local Anonymity in the Internet“. Boston University Computer Science Technical Report 97-002, 1998.
- [Menezes 1997] A. Menezes, P. van Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1997.
- [Micali 1992] S. Micali, P. Rogaway: „Secure Computation“. *Advances in Cryptology: Crypto '91*, Springer, 1992, S. 392–404.
- [Möller 1998] U. Möller: „Anonymisierung von Internet-Diensten“. Studienarbeit, Universität Hamburg, 12. Januar 1998.
- [Pfitzmann 1989] A. Pfitzmann, B. Pfitzmann, M. Waidner: „Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64+16)-kbit/s-Teilnehmeranschluß“. *Datenschutz und Datensicherung*, 13 (1989) 12, S. 605–622.

- [Pfitzmann 1990] A. Pfitzmann: *Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz*, Springer, 1990.
- [Pfitzmann 1990b] B. Pfitzmann, A. Pfitzmann: „How to Break the Direct RSA-Implementation of MIXes“. *Advances in Cryptology: Eurocrypt '89*, Springer, 1990, S. 373–381.
- [Rackoff 1993] C. Rackoff, D. Simon: „Cryptographic Defense Against Traffic Analysis“. *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing (STOC)*, ACM Press, 1993, S. 672–681.
- [Rannenberg 1995] K. Rannenberg et al.: „Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik“. H. Kubicek et al. (Hrsg.): *Jahrbuch Telekommunikation und Gesellschaft 1995*, v. Decker, 1995, S. 254–260.
- [Reed 1998] M. Reed, P. Syverson, D. Goldschlag: „Anonymous Connections and Onion Routing“. *IEEE Journal on Selected Areas in Communications*, 16 (1998) 4, S. 482–494.
- [Reiter 1997] M. Reiter, A. Rubin: „Crowds: Anonymity for Web Transactions“, DIMACS Technical Report 97-15, 1997.
- [Schneier 1996] B. Schneier: *Applied Cryptography*, 2. Auflage, Wiley, 1996.
- [Stevens 1998] W. R. Stevens: *UNIX Network Programming Volume 1*, 2. Auflage, Prentice Hall, 1998.
- [Stroustrup 1997] B. Stroustrup: *The C++ Programming Language*, 3. Auflage, Addison Wesley, 1997.
- [Wayner 1996] P. Wayner: *Disappearing Cryptography*, AP Professional, 1996.
- [Wiener 1998] M. Wiener: „Performance Comparison of Public-Key Cryptosystems“. *CryptoBytes*, 4 (1998) 1, 1998.
- [Wierda 1997] G. Wierda: „Release Notes for version 1.1 of the Squid cache“, 1997.
- [Young 1999] E. Young et al.: „OpenSSL“. URL: <http://www.openssl.org>
- [ZKS 1999] Zero Knowledge Systems, Inc.: „The Freedom Network Architecture (Version 1.0)“, 1999. URL: http://www.zks.net/products/Freedom_Architecture.html

[Zimmerman 1991] D. Zimmerman: „The Finger User Information Protocol“. *Internet RFC 1288*, Dezember 1991.

Index

- Angreifer, 13
 - aktiver, 26, 70
 - passiver, 22, 67
- anonyme Verbindungen, 31
- Anonymität, 14
 - perfekte, 14
- Anonymitätsmenge, 14
- Authentizität, 19

- Batch-Betrieb, 24
- Betriebsmodi, 16
- Blockchiffre, 16
- Browser, 8

- C++, 45
- CBC-Modus, *siehe* Betriebsmodi
- Client-Proxy, 44
- Cookies, 11
- Crowds, 36

- D_d , 15
- Data Encryption Standard (DES), 16
- Datenschutzanforderungen, 12
- denial-of-service-Angriff, 33
- DES, 61
- digitale Signaturen, 19
- Dummy-Nachricht, 24, 30
- Durchsatz, 63

- E_e , 15
- ECB-Modus, *siehe* Betriebsmodi
- Einwegfunktion, 17
- ElGamal, 18
- Empfänger-Anonymität, 14, 20, 35

- Flooding-Angriff, 29
- forward secrecy, 18
- Freedom, 38

- G , 25
- Hashfunktion, 19
- HMAC, 19, 50, 61
- HTTP, 8, 46
- Hybridverfahren, 18

- ideales Modell, 20
- informationstheoretische Sicherheit, 15, 36
- Inhaltsdaten, 13
- Integrität, 19, 28
- Internet Explorer, 10
- Isolieren von Nachrichten, 29
- IV, 16

- Jondo, 36

- Kanal, 51
- Kaskade, 23
- Kodierungsvorschrift, 18
- Konfusion, 25
- Kryptosystem, 15

- längentreue Umkodierung, 23
- lokale Anonymität, 36

- M_i , 21
- MAC, *siehe* Message Authentication Code
- Message Authentication Code, 19, 52
- Mix, 21
- Mix-Sequenz, 25

- Netscape Navigator, 10

- OAEP, 18, 61
- OpenSSL, 61
- Padding, 23, 28

Pakete, 51
Performanz, 63
personenbezogene Daten, 9
PGP, 49
plaintext awareness, 17
Proxy, 8, 45
Pseudonymität, 13
Pseudozufallszahlengenerator
(PRNG), 62
Public-Key-Verschlüsselung, *sie-
he* Verschlüsselungsver-
fahren, asymmetrische

Remailer, 21
Replay-Angriff, 22, 54
Reply-Block, 38
RSA, 17, 50, 61

Schlüssel
 öffentlicher, 17
 geheimer, 16
 privater, 17
Schlüsselverwaltung, 49
Sender-Anonymität, 14, 20
Server, 8
SHA-1, 19, 61
Sockets, 45
Stop-and-Go-Mixe, 24

traffic analysis, *siehe* Verkehrs-
analyse
Triple-DES, 16, 50

Umsortierung, 24
Unbeobachtbarkeit, 14
URL, 8

Verbindungsaufbaunachricht, 32
Verkehrsanalyse, 13, 33, 67
Verkehrsdaten, 13
Verschlüsselungsverfahren
 Angriffe, 16
 asymmetrische, 17
 probabilistische, 17
 Sicherheit, 15
 symmetrische, 16
Verzögerung, 24, 63
Wiederholungen, 22

WWW, 8, 35
Zertifizierungsinfrastruktur, 49
Zufallszahlen, 61

Ich erkläre hiermit, daß ich die vorliegende Arbeit selbständig erstellt und keine anderen als die angegebenen Hilfsmittel und Quellen verwendet habe.

Hamburg, den 16. Juli 1999

Electronic Patent Application Fee Transmittal

Application Number:	95001792				
Filing Date:	25-Oct-2011				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK				
First Named Inventor/Applicant Name:	7,188,180				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:	11519405
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	01-DEC-2011
Filing Date:	25-OCT-2011
Time Stamp:	11:54:23
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$400
RAM confirmation Number	11618
Deposit Account	081394
Authorized User	MCCOMBS,DAVID L

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		Petition_in_Opposition_to_Petition.pdf	755432 a50a3dddcd1d9c99b5fb4ead58884f5c922c09ed1	yes	16
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Receipt of Petition in a Reexam	1	15	
		Reexam Certificate of Service	16	16	
Warnings:					
Information:					
2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_A_Catalog_Listing_By_IBM.pdf	151828 fa153645651528035d1b2c88fee4f02bbccaf7111	no	4
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B_Page_From_217_Patent.pdf	79692 bc64db28a36b2b7b5839eb1bdcead443c29d247b	no	2
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_C_Pages_From_Security_Protocols.pdf	293877 dcafcf513317012653556e03eb2fbc357e9a5163	no	5
Warnings:					
Information:					
5	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D_Copy_Of_Search_Results_for_ISBN.pdf	86113 00d9ab80e82f2baa291466af80351a77651c1f9c4	no	2
Warnings:					
Information:					
6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_E_Catalog_Listing_from_BU_DC_Website.pdf	50137 f44099508482d6c8bac0a59df32ac9feac4f5f3	no	2
Warnings:					
Information:					
7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_F_Tec_Reports_Archive.pdf	383166 d6c23749e99114756be81a4d72c163cd3697303	no	6
Warnings:					
Information:					

8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_G_BU_Tech_Reports_Instru ctions.pdf	101515	no	3
			acb57efc628fb346eeea2b9234b8bc3ddbd c84c1		
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_H_U_Moller.pdf	4584033	no	84
			03f1813712ea1d1015e3ac28c48a23fbc057 086f		
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_I_Request_For_Comments_ 2026.pdf	1877665	no	37
			918fe3d4f728cea94aba22111c765bc250ba 3661		
Warnings:					
Information:					
11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_J_page_from_735_Patent. pdf	91751	no	2
			27698087bba3aa8bfa0b098d2b38bc58fc7 3f94		
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_K_page_from_053_Patent. pdf	95381	no	2
			a597c5f16aa4d051c94329ac6257f8910fad aa1		
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_L_page_from_989_Patent. pdf	71043	no	2
			d3452c5b9abfc6cb4b5fa77456f6e378d669 600c		
Warnings:					
Information:					
14	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_M_Link_to_RFC_1034.pdf	344881	no	6
			eeffc64a549eda360cb23e93e49d005a823a 38055		
Warnings:					
Information:					
15	Fee Worksheet (SB06)	fee-info.pdf	30698	no	2
			dc42776cab1452705c1b5e51cab6642fa2c 8e8d0		
Warnings:					
Information:					
Total Files Size (in bytes):			8997212		

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 <i>Inter Partes</i> Reexamination of:)	
)	
Victor Larson et al.)	Control No.: 95/001,792
)	
U. S. Patent No. 7,188,180)	Group Art Unit: 3992
)	
Issued: March 6, 2007)	Examiner: Karin M. Reichle
)	
For: METHOD FOR ESTABLISHING SECURE)	Confirmation No. 1972
COMMUNICATION LINK BETWEEN)	
COMPUTERS OF VIRTUAL PRIVATE)	
NETWORK)	

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

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 Petition to Vacate *Inter Partes* Reexamination was served by first-class mail on November 17, 2011, on counsel for the third party requester at the following address:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, TX 75219

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 17, 2011

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001792			
Filing Date:	25-Oct-2011			
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK			
First Named Inventor/Applicant Name:	7,188,180			
Filer:	Joseph Edwin Palys./Alison Evans			
Attorney Docket Number:	43614.100			
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:	11432505
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Alison Evans
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	17-NOV-2011
Filing Date:	25-OCT-2011
Time Stamp:	16:10:43
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$400
RAM confirmation Number	2965
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1		95_001792_PetitiontoVacate_1 1_17_11.pdf	47781 d3138c2021ed48e25c18f54b7384e79cb7ff 0ae3	yes	6
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Receipt of Petition in a Reexam	1	5	
		Reexam Certificate of Service	6	6	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30587 0d1fec829e9e295d60702c50e4162ff486a9 3616	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			78368		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor LARSON et al.) Control No.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Karin M. Reichle
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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

Sir:

NOTICE OF PRIOR AND CONCURRENT PROCEEDINGS

Pursuant to 37 C.F.R. § 1.985, VirnetX Inc., the patent owner, provides this notice of prior and concurrent proceedings. U.S. Patent No. 7,188,180 (the '180 patent), which is the subject of this proceeding, is currently at issue in the following litigation:

VirnetX Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America, and Aastra USA, Inc., No. 6:10-cv-00417 (E.D. Tex.).

The '180 patent was previously at issue in the following litigations, in which the parties reached a settlement agreement:

VirnetX Inc. v. Microsoft Corp., No 6:07-cv-00080 (E.D. Tex.);
and

VirnetX Inc. v. Microsoft Corp., No. 6:10-cv-00094 (E.D. Tex.).

The '180 patent was previously at issue in an *inter partes* reexamination proceeding filed by Microsoft Corporation on December 8, 2009 with Control No. 95/001,270.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 17, 2011

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.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Karin M. Reichle
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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

Sir:

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 Notice of Prior and Concurrent Proceedings was served by first-class mail on November 17, 2011, on counsel for the third party requester at the following address:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219-7672

Attorney Docket No. 11798.0005-00000
Control No. 95/001,792

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 17, 2011

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	11432637
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	22852
Filer:	Joseph Edwin Palys./Alison Evans
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	17-NOV-2011
Filing Date:	25-OCT-2011
Time Stamp:	16:15:55
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		95_001792_NoticePriorProceedings_11_17_11.pdf	34845 <small>c6a2da68e7879d8b695293cc628d5561b2e ea68f</small>	yes	4

Multipart Description/PDF files in .zip description		
Document Description	Start	End
Notice of concurrent proceeding(s)	1	2
Reexam Certificate of Service	3	4
Warnings:		
Information:		
Total Files Size (in bytes):		34845
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>		



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
95/001,792	10/25/2011	7,188,180	43614.100

CONFIRMATION NO. 1972

POA ACCEPTANCE LETTER

22852
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413



Date Mailed: 11/02/2011

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/01/2011.

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.

/kpdozier/

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
95/001,792	10/25/2011	7,188,180	43614.100

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

**CONFIRMATION NO. 1972
POWER OF ATTORNEY NOTICE**



Date Mailed: 11/02/2011

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/01/2011.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervned as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/kpdozier/

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

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,792	10/25/2011	7188180

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE , SUITE 700
DALLAS, TX 75219

CONFIRMATION NO. 1972
REEXAM ASSIGNMENT NOTICE



Date Mailed: 11/01/2011

NOTICE OF INTER PARTES REEXAMINATION REQUEST FILING DATE

Requester is hereby notified that the filing date of the request for *inter partes* reexamination is 10/25/2011, 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

/kpdozier/

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
95/001,792	10/25/2011	7188180

**CONFIRMATION NO. 1972
ASSIGNMENT NOTICE**

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096



Date Mailed: 11/01/2011

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
HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE , SUITE 700
DALLAS, TX 75219

/kpdozier/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor LARSON et al.) Control No.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Not Assigned
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
SECURE COMMUNICATION LINK)
BETWEEN COMPUTERS OF)
VIRTUAL PRIVATE NETWORK)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

**REVOCATION OF POWER OF ATTORNEY,
STATEMENT UNDER 37 C.F.R. § 3.73(b),
AND GRANT OF NEW POWER OF ATTORNEY
FOR REEXAMINATION CONTROL NO. 95/001,792 ONLY**

The undersigned, a representative authorized to sign on behalf of the assignee owning all of the interest in U.S. Patent No. 7,188,180 ("the '180 patent"), hereby revokes all previous powers of attorney or authorization of agent granted only in the above-mentioned reexamination proceeding, i.e., control no. 95/001,792.


As required by 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 '180 patent by virtue of assignments recorded in the U.S. Patent and Trademark Office at Reel/Frame 014679/0947 and 018757/0326.

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 prosecute only reexamination proceeding with control no. 95/001,792 and to transact all business in the Patent and Trademark Office connected therewith. Power of attorney and the mailing address for all other aspects of the '180 patent shall remain unchanged.

Please send all future correspondence concerning reexamination proceeding with control no. 95/001,792 to Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Customer No. 22,852.

Dated: November 1, 2011

By: 
Sameer Mathur
VP of Corporate Development
and Product Marketing
Virnetx Inc.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
)
Victor LARSON et al.) Control No.: 95/001,792
)
U. S. Patent No. 7,188,180) Group Art Unit: 3992
)
Issued: March 6, 2007) Examiner: Not Assigned
)
For: METHOD FOR ESTABLISHING) Confirmation No. 1972
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

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 Revocation of Power of Attorney, Statement Under 37 C.F.R. §3.73(b), and Grant of New Power of Attorney for Reexamination Control No. 95/001,792 was served by first-class mail on November 1, 2011, on counsel for the third party requester at the following address:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 1, 2011

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	11312144
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7,188,180
Customer Number:	23630
Filer:	Joseph Edwin Palys./Alison Evans
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.100
Receipt Date:	01-NOV-2011
Filing Date:	25-OCT-2011
Time Stamp:	16:07:15
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		20111101POA_0005.pdf	123216 40972c49e6b7867c21c19b6374b3a68e117537ab	yes	3

Multipart Description/PDF files in .zip description		
Document Description	Start	End
Power of Attorney	1	2
Reexam Certificate of Service	3	3

Warnings:

Information:

Total Files Size (in bytes):	123216
-------------------------------------	--------

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



Bib Data Sheet

CONFIRMATION NO. 1972

SERIAL NUMBER 95/001,792	FILING OR 371(c) DATE 10/25/2011 RULE	CLASS 709	GROUP ART UNIT 3992	ATTORNEY DOCKET NO. 43614.100
------------------------------------	---	---------------------	-------------------------------	---

APPLICANTS

7,188,180, Residence Not Provided;
 VIRNETX INC. (OWNER), SCOTTS VALLEY DRIVE, CA;
 HAYNES AND BOONE, LLP (3RD.PTY.REQ.), DALLAS, TX;
 CISCO SYSTEMS, INC. (REAL.PTY.IN.INTEREST.), Residence Not Provided;
 HAYNES AND BOONE, LLP, DALLAS, TX

**** CONTINUING DATA *******

This application is a REX of 10/702,486 11/07/2003 PAT 7,188,180
 which is a DIV of 09/558,209 04/26/2000 ABN
 which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
 which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
 which claims benefit of 60/106,261 10/30/1998
 and claims benefit of 60/137,704 06/07/1999

**** FOREIGN APPLICATIONS *******

Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> 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:	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees (Filing)
		<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)
		<input type="checkbox"/> 1.18 Fees (Issue)
		<input type="checkbox"/> Other _____
		<input type="checkbox"/> Credit _____

Patent Assignment Abstract of Title

Total Assignments: 2

Application #: 10702486 **Filing Dt:** 11/07/2003 **Patent #:** 7188180 **Issue Dt:** 03/06/2007
PCT #: NONE **Publication #:** US20040107285 **Pub Dt:** 06/03/2004
Inventors: Victor Larson, Robert Dunham Short III, Edmund Colby Munger, Michæl Williamson
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATÉ NETWORK

Assignment: 1

Reel/Frame: 014679 / 0947 **Received:** 11/14/2003 **Recorded:** 11/07/2003 **Mailed:** 06/03/2004 **Pages:** 3

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: BANNER & WITCOFF, LTD.
ROSS A. DANNENBERG
1001 G STREET, N.W., 11TH FLOOR
WASHINGTON, DC 20001

Assignment: 2

Reel/Frame: 018757 / 0326 **Received:** 01/10/2007 **Recorded:** 01/10/2007 **Mailed:** 01/16/2007 **Pages:** 5

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 DRIVE, CALIFORNIA 95066

Correspondent: BANNER & WITCOFF, LTD.
1001 G STREET, N.W. - 11TH FLOOR
WASHINGTON, D.C. 20001-4597

Search Results as of: 10/31/2011 08:04 AM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.1.1
Web interface last modified: Aug 19, 2011

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.: 43614.100Date: October 25, 2011

1. This is a request for *inter partes* reexamination pursuant to 37 CFR 1.913 of patent number 7,188,180 issued March 6, 2007. The request is made by a third party requester, identified herein below.
2. a. The name and address of the person requesting reexamination is:
David L. McCombs,
Haynes and Boone, LLP, 2323 Victory Avenue, Suite 700
Dallas, Texas 75219
- b. The real party in interest (37 CFR 1.915(b)(8)) is: Cisco Systems, Inc.
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. _____ ; **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. 08-1394 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) 1-41 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.

[Page 1 of 2]

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.

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.

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:
McDermott Will & Emery
600 13th Street, NW
Washington DC 20005-3096
 Date of Service: October 25, 2011; 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: 27683

OR

Firm or Individual Name _____

Address _____

City	State	Zip
Country		
Telephone <u>214-651-5533</u>	Email <u>ipdocketing@haynesboone.com</u>	

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, Case No. 6:10-cv-417
(E.D. Tex. filed Aug. 11, 2010).

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.

<u>/David L. McCombs/</u>	<u>October 25, 2011</u>
Authorized Signature	Date
<u>David L. McCombs</u>	<u>32,271</u>
Typed/Printed Name	Registration No., if applicable

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

In place of PTO-1449 Form		U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Application Number	Inter Partes Reexamination of U.S. Patent No. 7,188,180
				Filing Date	October 25, 2011
				Real Parties in Interest	Cisco Systems, Inc.
				Art Unit	TBD
				Examiner Name	TBD
SHEET	1	OF	1	Attorney Docket Number	43614.100

U. S. PATENTS				
Examiner's Initials	Cite No.	Document Number	Issue Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

U. S. PATENT APPLICATION PUBLICATIONS				
Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	Cite No.	Foreign Patent Document (Country Code - Number - Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	Exhibit D1	ROLF LENDENMANN, "UNDERSTANDING OSF DCE 1.1 FOR AIX AND OS/2, IBM International Technical Support Organization" (Oct. 1995).
	Exhibit D2	TAKAHIRO KIUCHI AND SHIGEKOTO KAIHARA, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," published in the Proceedings of SNDSS 1996.
	Exhibit D3	EDUARDO SOLANA AND JÜRGEN HARMS, "Flexible Internet Secure Transactions Based on Collaborative Domains," Security Protocols Workshop 1997, pp. 37-51.
	Exhibit D4	DAVID M. MARTIN, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).
	Exhibit D5	BRUCE SCHNEIER, "APPLIED CRYPTOGRAPHY" (1996).
	Exhibit D7	BRIAN C. SCHIMPF, "Securing Web Access with DCE," presented at Network and Distributed System Security (Feb. 10-11, 1997).
	Exhibit D8	WARD ROSENBERY, DAVID KENNEY, AND GERRY FISHER, "UNDERSTANDING DCE" (1993).
	Exhibit D9	DANIEL R. MASYS & DIXIE B. BAKER, "Protecting Clinical Data on Web Client Computers: the PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, FL (Nov. 7-11, 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 a copy of this form with next communication to applicant.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Larson et al.

U.S. Patent No. 7,188,180

Filed: November 7, 2003

Issued: Mar. 6, 2007

Title: METHOD FOR ESTABLISHING
SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF VIRTUAL
PRIVATE NETWORK

§ REQUEST FOR *Inter Partes*
§ REEXAMINATION

§ Attorney Docket No.: 43614.100

§ Customer No.: 27683

§ Real Party in Interest:
§ Cisco Systems, Inc.

REQUEST FOR INTER PARTES REEXAMINATION

Mail Stop *Inter partes* Reexam
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to the provisions of 35 U.S.C. §§ 311-318, David L. McCombs (“Requester”) hereby requests *inter partes* reexamination of claims 1-41 (all of the claims) of United States Patent No. 7,188,180 that issued on March 6, 2007, to Larson et al. (“the ‘180 patent,” Ex. A), on behalf of Cisco Systems, Inc., the real party in interest. In accordance with 37 C.F.R. § 1.915(b)(7), Cisco Systems, Inc. hereby certifies that the estoppel provisions of 37 C.F.R. § 1.907 do not prohibit this request for *inter partes* reexamination.

This request presents prior art references that are better than and non-cumulative of the prior art that was considered during the original prosecution of the ‘180 patent or in earlier reexamination control no. 95/001,270. Claims 1-41 (all of the claims) are invalid over these new references. Requester asks that reexamination be ordered and that all of the claims be rejected and ultimately canceled.

The ‘180 patent is also the subject of pending litigation, styled *VirnetX, Inc. v. Cisco Systems, Inc.*, Case No. 6:10-cv-417 (E.D. Tex. filed Aug. 11, 2010). No final decision has been entered in that case.

TABLE OF CONTENTS

I. Introduction	3
II. Description and File History of the '180 Patent	4
A. Prosecution of the Parent U.S. App. 09/558,209	5
B. Prosecution of the '180 Patent	5
C. Related Patents	7
D. Prior Reexamination of the '180 Patent	9
E. The Effective Priority Date of the Claims in the '180 Patent	11
III. Newly Cited Prior Art Demonstrates a Reasonable Likelihood that Requester Will Prevail With Respect to Claims 1-41	12
A. Lendenmann	12
B. Kiuchi	15
C. Solana	17
D. Schimpf	19
IV. Detailed Explanation of the Pertinency and Manner of Applying the Prior Art to the Claims	20
A. Summary of the Additional Prior Art	20
(i) RFC 793	21
(ii) Masys	21
(iii) Martin	21
(iv) Rosenberry	21
(v) Schneier	22
(vi) RFC 1034	22
B. Statutory Bases for Proposed Rejections of the Claims	22
C. Proposed Rejections of the Claims	23
(a) Proposed Rejections Based on Lendenmann	23
(b) Proposed Rejections Based on Kiuchi	23
(c) Proposed Rejections Based on Solana	24
(d) Proposed Rejections Based on Schimpf and Rosenberry	24
D. Claim Interpretation	24
V. List of Exhibits	25
VI. Conclusion	27
VII. Certificate of Service	28

I. Introduction

U.S. Patent 7,188,180 describes a method for accessing a secure computer network address that corresponds to a secure domain name. Previously unknown to the Patent Office, such technology had been developed and publicized by others more than a year before the patent's earliest claimed priority date. This request shows how newly presented references, alone or in combination with other references, invalidate claims 1-41 of the '180 patent. As detailed below and in the claim chart exhibits, this request shows a reasonable likelihood that requester will prevail with respect to claims 1-41 of the patent.

In a previous reexamination of the '180 patent, the Patent Owner overcame numerous prior art rejections by arguing that the claimed "secure domain name" is not a domain name that corresponds to a secure computer. Rather, the Patent Owner asserted (and the prior reexamination examiner agreed) that a *secure domain name* is a name that "cannot be resolved by a conventional domain name service."¹ The Patent Owner further argued that only a "secure domain name service" could resolve such secure domain names. On the basis of these arguments, the reexamination examiner confirmed the claims.

But prior art publications not available to the reexamination examiner teach using secure domain names that cannot be resolved by a conventional domain name service. For example, the Lendenmann reference describes a network architecture for providing secure, authenticated, and authorized communications between clients and servers. The architecture includes an integrated directory server that responds to authorized requests for computer network addresses that correspond to both conventional and secure domain names. A client then sends an encrypted request to the server at the network address received from the directory server. The server verifies the client's authorization to receive a requested service. Thus, Lendenmann teaches accessing a secure computer network address that corresponds to a secure domain name.

Another reference, Kiuchi, describes how a client sends a domain name request to a secure name server. The secure name server responds with the target computer's address and encryption key. The client then sends a request to communicate securely with the target computer using the encryption key. Thus, Kiuchi teaches a method for accessing a secure

¹ Reexamination Control No. 95/001,270, Response at 6 (May 24, 2010).

computer network address that corresponds to a secure domain name via a virtual private network.

Still other references, such as Solana and Schimpf, describe non-conventional domain name services that enable secure, authenticated communications over the Internet.

These references provide new, non-cumulative disclosures of the features recited in the '180 patent claims. They invalidate the claims.

Requester therefore asks that the Office issue an Order for Reexamination and that the reexamination proceed to reject and cancel claims 1-41 of the '180 Patent.

II. Description and File History of the '180 Patent

U.S. 7,188,180 was filed November 7, 2003, as application no. 10/702,486. The '180 patent is a divisional of application no. 09/558,209, filed Apr. 26, 2000, now abandoned, which is a continuation-in-part of application no. 09/504,783, filed Feb. 15, 2000, now issued as U.S. 6,502,135 (attached as Exhibit C-1), which is itself a continuation-in-part of application no. 09/429,643, filed Oct. 29, 1999, now issued as U.S. 7,010,604 (attached as Exhibit C-2). The '180 patent claims priority to these earlier applications. The last of these, U.S. 7,010,604, claims the benefit of provisional application No. 60/106,261, filed on October 30, 1998 (attached as Exhibit C-3), and provisional application No. 60/137,704, filed on June 7, 1999 (attached as Exhibit C-4).

The '180 patent has 41 total claims and three independent claims—claims 1, 17, and 33. Claim 1 describes a method for accessing a secure computer network address, while claims 17 and 33 are directed to a storage medium (claim 17) or an apparatus (claim 33) with instructions for performing substantially the same method. Thus, the body of each claim recites method steps.

Claim 1 is representative:

1. A method for accessing a secure computer network address, comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

Relevant aspects of the file history include the prosecution of the parent U.S. App. 09/558,209 (attached as Exhibit B-2) and the prosecution of the '180 patent itself (attached as Exhibit B-1).

A. Prosecution of the Parent U.S. App. 09/558,209

U.S. patent application no. 09/558,209 was filed Apr. 26, 2000 with 116 claims. In a preliminary amendment filed Feb. 26, 2002, the applicants amended certain claims and added two additional claims “to more broadly claim the disclosed invention.”² In the first Action, the Examiner entered a three-way Restriction Requirement.³ Group II, with claims 31-52 and 117-18, generally correspond to the claims that later issued in the '180 patent. The Applicants did not choose Group II. Instead, the Applicants elected without traverse Group I, corresponding to claims 1-30.⁴

The Examiner then issued a Notice of Allowance.⁵ The applicants did not pay the issue fee, and a Notice of Abandonment was mailed on Dec. 23, 2003.⁶

B. Prosecution of the '180 Patent

U.S. 7,188,180 was filed November 7, 2003, as application no. 10/702,486. The '180 patent is a divisional of application no. 09/558,209. The application-as-filed included 24 claims.

In a first Office action dated May 19, 2006, the examiner rejected claims 1 and 2 as being indefinite under 35 U.S.C. § 112, second paragraph. The examiner noted the claims failed to indicate where various steps of the method were performed:⁷

² File History of U.S. App. 09/558,209, Amendment at 3 (Feb. 26, 2002).

³ File History of U.S. App. 09/558,209, Office Action at 2 (Jul. 3, 2003).

⁴ File History of U.S. App. 09/558,209, Election and Response (Aug. 4, 2003).

⁵ File History of U.S. App. 09/558,209, Notice of Allowance at 2-3 (Aug. 12, 2003).

⁶ File History of U.S. App. 09/558,209, Notice of Abandonment (Dec. 23, 2003).

⁷ File History of U.S. 7,188,180, Office Action at 2 (May 19, 2006).

In claim 1, line 3, it is unclear from a query message is sent. At line 4, it unclear from the query message is requesting a secure computer network address.

At line 5, it is unclear where the response message is received and from where is the response message is received. At line 7, It is unclear from where an access request is sent.

The Examiner also stated that prior art not relied upon but considered relevant to the Applicants' disclosure "are cited in the Form PTO-892 for the applicant's review."⁸ The form, however, was essentially blank and did not cite any prior art references.

In response, the Applicants amended claim 1 to specifically recite that the query message requests information from the secure domain name service, which the provides the response message:⁹

1. (Currently Amended) A method for accessing a secure computer network address, comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.

The Applicants also argued that "where the method is embodied is unclaimed, and thus immaterial with respect to claim 1."¹⁰ The Applicants added new claims 25-41.

The Examiner then issued a Notice of Allowance with the following statement of reasons for allowance:

⁸ File History of U.S. 7,188,180, Office Action at 2 (May 19, 2006).

⁹ File History of U.S. 7,188,180, Response at 3 (Aug. 17, 2006).

¹⁰ File History of U.S. 7,188,180, Response at 10 (Aug. 17, 2006).

The prior arts of record do not teach a system and a method for accessing a secure computer network address comprising steps of: requesting a secure computer network address from a secure domain name server according to the secure domain name; and using a virtual private network communication link to send an access request message to the secure computer network address.

The examiner considers the applicants' claims 1-41 to be allowable based on the claim interpretation and the aforesaid prior arts of record.

Although the Notice of Allowance referred to "aforesaid prior arts of record," the Notice did not cite or discuss any prior art references.

In summary, the claims of the '180 patent were never rejected based on prior art, and the examiner did not identify or discuss any prior art references believed to be relevant to the claims.

C. Related Patents

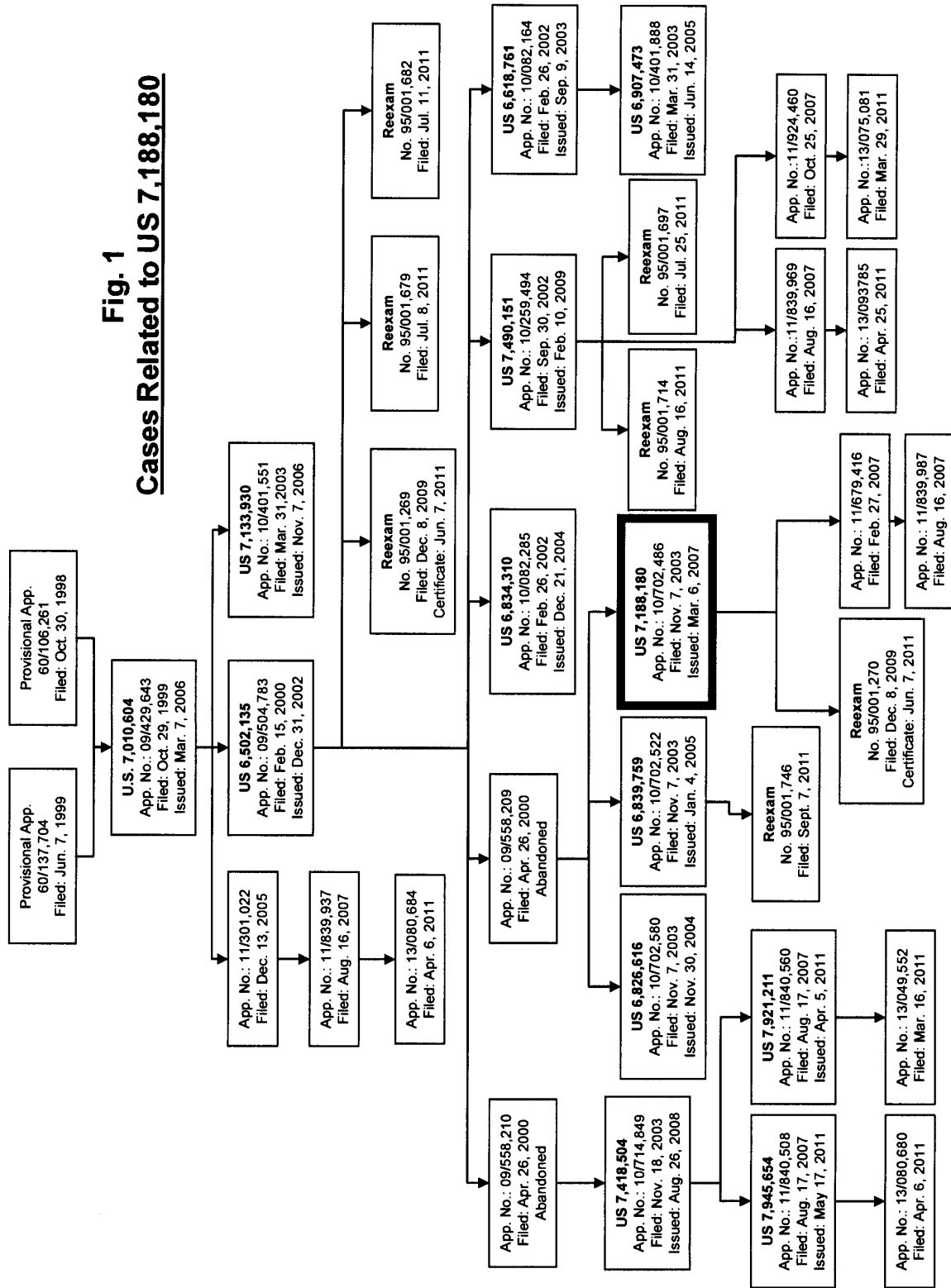
The '180 patent is part of a patent family that includes the parent patents and patent applications through which it claims priority, along with other related patents and patent applications. Various patent applications in the family are pending at the Patent Office, while some issued patents in the family are the subject of pending or completed reexamination proceedings.

In particular, the Requester notes that the following related patents are the subject of currently pending *inter partes* reexamination requests or proceedings:

Patent No.	Reexam Control No.	Request Filed
6,502,135	95/001,679	Jul. 8, 2011
	95/001,682	Jul. 11, 2011
7,490,151	95/001,714	Aug. 16, 2011
	95/001,697	Jul. 25, 2011
6,839,759	95/001,746	Sept. 7, 2011

Requester has summarized the patents and applications related to the '180 patent in the Figure 1 below based on the information on these cases that is publicly available.

Fig. 1
Cases Related to US 7,188,180



D. Prior Reexamination of the '180 Patent

The '180 patent was the subject of *inter partes* Reexamination Control No. 95/001,270 requested by Microsoft Corporation. The Patent Office found that the new prior art references in Microsoft's request raised substantial new questions of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35.¹¹

In the first Office Action, the examiner adopted numerous proposed anticipation and obviousness rejections based on the submitted prior art references.¹²

The Patent Owner argued that it was improper for the Patent Office to interpret the term "secure domain name" as broadly as a federal court had in the Patent Owner's co-pending litigation against Microsoft.¹³ Specifically, the Patent Owner argued that the "Request and Office Action rely on the erroneous premise that a secure domain name is a domain name that happens to correspond to a secure computer."¹⁴ Instead, the Patent Owner asserted that a secure domain name is a name that "cannot be resolved by a conventional domain name service."¹⁵ Similarly, the Patent Owner argued that the claim term "secure domain name service" should be understood to refer to something "different from a conventional domain name service."¹⁶

Microsoft subsequently filed a Notice of Non-Participation, indicating that it had settled with the Patent Owner and would not participate further in the *inter partes* reexamination.¹⁷

The Examiner then issued an Action Closing Prosecution with all claims confirmed. The Examiner stated that "the '180 patent clearly distinguishes the claimed 'secure domain name' from a domain name that happens to correspond to a secure computer."¹⁸ The Examiner

¹¹ Reexamination Control No. 95/001,270, Order Granting Reexamination Request at 6-12 (Jan. 19, 2010).

¹² Reexamination Control No. 95/001,270, Office Action at 5-27 (Jan. 19, 2010).

¹³ The court had construed the term secure domain name to mean "a domain name that corresponds to a secure computer network address." *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009).

¹⁴ Response at 5 (Apr. 19, 2010).

¹⁵ *Id.* at 6.

¹⁶ *Id.* at 8.

¹⁷ Third Party Requester's Notice of Non-Participation (May 18, 2010).

¹⁸ Reexamination Control No. 95/001,270, Action Closing Prosecution at 3 (Jun. 16, 2010).

explained that a secure domain name cannot be resolved by a conventional domain name service.¹⁹

connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains 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, column 51 lines 25-35).

On that basis, the Examiner withdrew all of the earlier rejections.²⁰ The Examiner provided the following statement of reasons for confirmation:²¹

Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed as patentable for the following reasons. The cited prior art fails to teach or suggest the claimed features of a "secure domain name" and a "secure domain name service." Instead, the cited prior art teaches the use of a conventional domain name system and conventional domain names where some of the domain names correspond to a host that requires authentication. 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 domain name server using a secure domain name will result in a return

¹⁹ Reexamination Control No. 95/001,270, Action Closing Prosecution at 3 (Jun. 16, 2010).

²⁰ See generally *id.* at 14-23.

²¹ *Id.* at 13-14.

message indicating that the URL is unknown ('180 patent, column 51 lines 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, column 51 lines 25-35). Accordingly, the cited prior art fails to anticipate or render obvious claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35.

Thus, the file history indicates that the prosecution and reexamination Examiners would have been interested in a prior art reference that described a secure domain name server capable of resolving addresses for secure domain names that cannot be resolved by a conventional domain name service.

E. The Effective Priority Date of the Claims in the '180 Patent

As noted above, the '180 patent was filed November 7, 2003 but claims priority as far back as provisional application no. 60/106,261, filed Oct. 30, 1998.

Each of the independent claims in the '180 patent (claims 1, 17, and 33) includes limitations that have their earliest possible written description support in the continuation-in-part application no. 09/558,209, filed April 26, 2000. For example, each independent claim recites "sending a query message to a secure domain name service."

To the extent there is any written description support for this limitation, the written description support for this claimed subject matter first appeared in the '209 CIP application filed on April 26, 2000. The '209 application includes a section specifically labeled "CONTINUATION-IN-PART IMPROVEMENTS," starting at page 56 of the originally-filed specification. For example, the description on pages 81–88 discusses "querying a secure domain name service (SDNS)."²²

None of the earlier-filed applications include corresponding descriptions of the claimed functionality. Indeed, the earlier-filed applications do not even discuss to domain names, let alone secure domain names. Accordingly, the *effective* priority date of independent claims 1, 17, and 33 (and, by dependency, all of the other claims) is April 26, 2000. As previously noted, the earliest *claimed* priority date is October 30, 1998.

²² File History of U.S. App. 09/558,209, Specification as-filed at 84.

III. Newly Cited Prior Art Demonstrates a Reasonable Likelihood that Requester Will Prevail With Respect to Claims 1-41

As discussed above, the record states that claims of the '180 patent were confirmed in the previous reexamination because the prior art considered in that proceeding failed to teach a secure domain name that could not be resolved by a conventional domain name service. As shown below, the references presented in this request teach this limitation. Because these references provide technical disclosures that the Examiner believed to be absent in the prior art, the references are not cumulative of art already considered by the Office. Their teachings—as explained below and detailed more fully in the attached claim charts—demonstrate a reasonable likelihood that the Requester will prevail with respect to claims 1-41 of the '180 patent.

A. Lendenmann

“Understanding OSF DCE 1.1 for AIX and OS/2” by Ralf Lendenmann (“Lendenmann”), was published by the IBM International Technical Support Organization in October 1995. This publication was publicly available more than one year before the '180 Patent’s earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of Lendenmann is attached as Exhibit D-1. Lendenmann has not been previously cited to the Patent Office.

Lendenmann describes the Distributed Computing Environment (DCE) software system that provides a broad set of name resolution, security, and remote access features for computer networks. Specifically, Lendenmann teaches that the naming services in DCE provide name resolution services for both conventional (Internet DNS) and non-conventional (CCITT X.500) domain names:²³

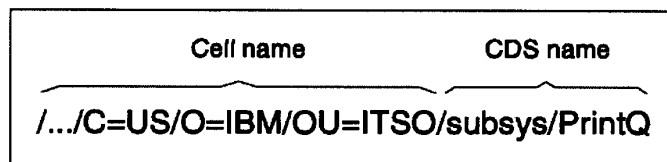
There are two well-established naming schemes in place that DCE makes use of:

- CCITT X.500
- Internet Domain Name Service (DNS)

As the examples in Lendenmann make clear, the CCITT X.500 naming scheme provides names that *could not* be resolved by a conventional domain name service. For example, such names do

²³ Lendenmann at 23.

not end in any of the standard domain names “.com, .net, .org, .edu, .mil or .gov.”²⁴ An example name is shown in Lendenmann Fig. 9 below:

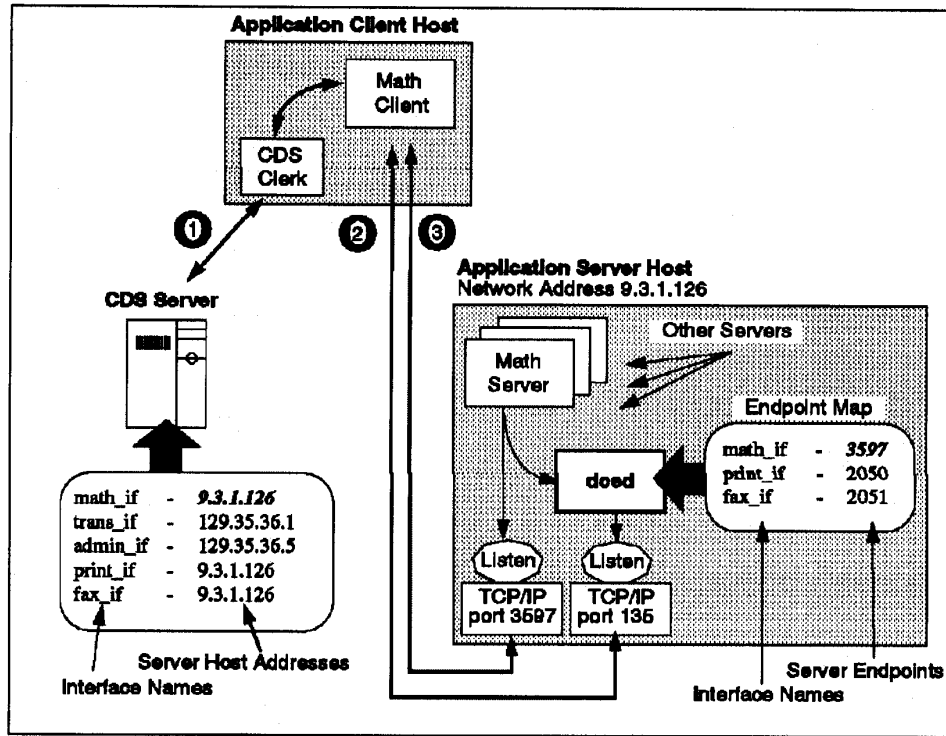


Lendenmann Fig. 9

Lendenmann further teaches initiating a virtual private network communication link with the network address associated with such a secure domain name. For example, Lendenmann illustrates in Fig. 68 a three-step process for initiating a remote procedure call (RPC) from a client to a server:

1. Obtaining the network address for the requested service from the CDS server.
2. Contacting the server to obtain the port number for a specific service.
3. Submitting the remote procedure call (RPC) request to the server at the designated port number.

²⁴ '180 Patent, 50:18.



Lendenmann Fig. 68

Lendenmann specifically teaches that performing a remote procedure call (RPC) includes providing authenticated and encrypted communication between a client and a server. For example, both the “CDMF Privacy” and “Packet Privacy” options provide encryption for authenticated RPC communications between the client and server:²⁵

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. As a rule, the more restrictive the protection level, the greater the impact on performance.

The following protection levels are available:

- None. No communication protection.

²⁵ Lendenmann at 192.

- **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.

These private, encrypted communications provide a virtual private network between the client and server.

In summary, Lendenmann teaches a client that obtains a server's network address by querying a secure domain name service to resolve a name that could not be resolved by a conventional domain name service. Lendenmann further teaches establishing a virtual private network between the client and server. Thus, Lendenmann provides a better disclosure than (and is not cumulative of) the references previously considered by the Patent Office. As detailed more specifically in the claim chart attached as Exhibit E-1, Lendenmann teaches all of the limitations of claim 1. And alone or in combination with other references, Lendenmann teaches all of the limitations of claims 2-41. Thus, Lendenmann demonstrates a reasonable likelihood that the Requester will prevail with respect to claims 1-41.

B. Kiuchi

“C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet” by Takahiro Kiuchi and Shigekoto Kaihara (“Kiuchi”) was published in the Proceedings of the Symposium on Network and Distributed System Security, 1996. This publication was publicly available more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of Kiuchi is attached as Exhibit D-2. Kiuchi has not been previously cited to the Patent Office.

Similar to the '180 patent, Kiuchi was concerned with establishing secure network links between computers. Kiuchi sought to develop a secure network by which medical information,

including sensitive clinical trial documents, could be easily shared between different hospitals and other institutions.

To accomplish this goal, Kiuchi describes a system with “a client-side proxy, a server-side proxy and a C-HTTP name server.”²⁶ The proxies reside on a firewall computer and “communicate with each other using a secure, encrypted protocol.”²⁷ Thus, the communications between proxies use an encrypted channel.

Kiuchi teaches that a client-side proxy initiates a secure connection by first sending a request to the C-HTTP name server for the IP address of a specified server-side proxy. After the C-HTTP name server responds with the IP address, the client-side proxy sends an encrypted connection request message to the server-side proxy:

*A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL.... If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values.... When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client-side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy's public key....*²⁸

Kiuchi expressly teaches that the server names resolved by the C-HTTP name server are *not* conventional domain names:

In a C-HTTP-based network, *instead of a DNS*, a C-HTTP-based secure, encrypted name and certification service is used.²⁹

For example, Kiuchi provides example names for the client-side proxy and server-side proxy that are not conventional domain names:³⁰

²⁶ Kiuchi, Abstract.

²⁷ Kiuchi, Abstract.

²⁸ Kiuchi, p. 65 (emphasis added).

²⁹ Kiuchi, p. 64 (emphasis added).

³⁰ Kiuchi, p. 73.

- 1) Client-side proxy
hostname: University.of.Tokyo.Branch.Hospital
IP address: 130.69.111.111
- 2) server-side proxy
hostname: Coordinating.Center.CSCRG
IP address: 130.69.222.222
port number: 8080

Kiuchi's example domain names end in ".Hospital" and ".CSCRG", whereas the '180 patent states that standard domain names end instead in ".com, .net, .org, .edu, .mil or .gov."³¹ Thus, the domain names taught by Kiuchi are *not* conventional domain names that could be resolved by a conventional domain name service.

Kiuchi further teaches that the secure, encrypted connection is a virtual private network communication link as recited in the '180 patent claims. For example, Kiuchi describes the secure connections among computers as forming a "closed HTTP-based *virtual network*" that serves as a more flexible alternative to privately leased circuits.³²

In summary, Kiuchi teaches a secure domain name service that resolves names that could not be resolved by a conventional domain name service. Kiuchi further teaches establishing a virtual private network with a secure network address identified by a secure domain name. Thus, Kiuchi provides a better disclosure than (and is not cumulative of) the references previously considered by the Patent Office. As detailed more specifically in the claim chart attached as Exhibit E-2, Kiuchi teaches all of the limitations of claim 1. And alone or in combination with other references, Kiuchi teaches all of the limitations of claims 2-41. Thus, Kiuchi demonstrates a reasonable likelihood that the Requester will prevail with respect to claims 1-41.

C. Solana

"Flexible Internet Secure Transactions Based on Collaborative Domains," by Eduardo Solana and Jürgen Harms ("Solana") was presented at the Security Protocols Workshop held April 7-9, 1997 in Paris. This publication was publicly available more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. §

³¹ '180 Patent, col. 50, l. 18.

³² Kiuchi, p. 69.

102(b). A copy of Solana is attached as Exhibit D-3. Solana has not been previously cited to the Patent Office.

Solana describes a security architecture for providing encrypted, authenticated communications over the Internet. For example, Solana describes techniques for “transparent secure gatewaying between domains and end-to-end secure transactions.”³³ Solana further describes a global Directory Service (DS) that uses an X.509 naming infrastructure and stores network addresses, among other data.³⁴

A coordinated, global *Directory Service* (DS) holding naming information and especially certificates that securely bind domains to their public keys is also required and constitutes the cryptographic support for inter-domain transactions. As mentioned, existing naming infrastructures (DNS-sec, X.509) might be used for this purpose.

A well defined convention establishing an *Uniform Naming Information* (UNI) is also needed to designate principals and domains globally and unequivocally as, for instance, a common name, an E-mail address, or a network address. Note that this information may also be published in the Directory Service.

This global Directory Service (DS) using the X.509 naming infrastructure is capable of resolving domain names that could not be resolved by a conventional domain name service. Thus, the global Directory Service (DS) is a secure domain name service.

Solana further teaches that an initiator queries the global Directory Service (DS) and then sends an encrypted request to a responder.³⁵

1. The initiator generates the same header as in the precedent case (Session Key + responder UNI) and then issues a DS query to obtain the destination domain public key for header encryption. Finally, the whole packet together with the decryption information is submitted directly to the responder.

This private, encrypted communication provides a virtual private network between the initiator and responder.

In summary, Solana teaches an initiator that obtains a responder’s network address by querying a global Directory Service (DS) that resolves a name that could not be resolved by a

³³ Solana at 48, emphasis added.

³⁴ Solana at 43.

³⁵ Solana at 46.

conventional domain name service. Solana further teaches establishing a virtual private network between the initiator and responder. Thus, Solana provides a better disclosure than (and is not cumulative of) the references previously considered by the Patent Office. As detailed more specifically in the claim charts attached as Exhibit E-3, Solana teaches all of the limitations of claim claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35. Thus, Solana demonstrates a reasonable likelihood that the Requester will prevail with respect to these claims.

D. Schimpf

Schimpf is “Securing Web Access with DCE,” by Brian C. Schimpf, presented at Network and Distributed System Security, Feb. 10-11, 1997. This publication was publicly available more than one year before the ’180 Patent’s earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of Schimpf is attached as Exhibit D-7. Schimpf has not been previously cited to the Patent Office.

Schimpf describes providing encrypted and authenticated access to specialized servers from an ordinary web browser. Specifically, Schimpf describes providing a Secure Local Proxy (SLP) that intercepts web page requests and determines whether the request is directed to an ordinary web site or, alternatively, to a Distributed Computing Environment (DCE) Cell Directory Service (CDS) object name. If to a DCE name, then the request is tunnel through an authenticated, encrypted remote procedure call to the secure server:³⁶

2.1.1 Client. The client is the leftmost box in Figure 1 and consists of a standard, off-the-shelf Web browser, running on a desktop system. In addition to the browser, DCE runtime services are installed on the system, as is a component called the Secure Local Proxy (SLP). The SLP intercepts all HTTP requests from the browser using a standard browser proxy mechanism. If the request is for a normal Web access the request is forwarded directly to the Web server using HTTP. The SLP can be configured to forward the request to another proxy process if required. If, on the other hand, the request is for a DCE-enabled Web access, determined by the presence of a DCE CDS object name in the URL, the SLP locates an appropriate

³⁶ Schimpf at 105.

DCE-aware Web server to fulfill the request using DCE naming services. The SLP then “tunnels” the request to that server by wrapping the HTTP request in a secure DCE RPC. The SLP is therefore a DCE client. This will typically be an authenticated DCE interaction and the proper DCE authorization information, specifically a DCE PAC (privilege attribute certificate), will be transferred with the request. This DCE interaction can be configured to use either no security, authentication only or authentication plus privacy (i.e., encryption) protection. By choosing privacy protection the DCE RPC access between the SLP and the application server is encrypted prior to transmission in either direction, thus protecting the information exchanged from observers with access to network traffic.

The authenticated, encrypted remote procedure call also includes the client’s authorization information. Thus, the remote procedure call is a virtual private network.

Since the SLP is able to distinguish between a “normal Web access” and a request that should be tunneled via a secure remote procedure call, it is apparent that the SLP is able to distinguish between conventional domain names and secure domain names. In addition, the SLP is aware of and recognizes the need to provide secure treatment of the secure domain names.

In summary, Schimpf teaches a client with a web browser and an interceptor that recognizes the presence of a secure domain name in a web browser request. Schimpf further teaches establishing a virtual private network between the client and a secure server. Thus, Schimpf provides a better disclosure than (and is not cumulative of) the references previously considered by the Patent Office. As detailed more specifically in the claim charts attached as Exhibit E-4, Schimpf in combination with other references renders obvious all of the limitations of claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35. Thus, Schimpf demonstrates a reasonable likelihood that the Requester will prevail with respect to these claims.

IV. Detailed Explanation of the Pertinency and Manner of Applying the Prior Art to the Claims

A. Summary of the Additional Prior Art

This request relies on additional prior art references to propose obviousness rejections in combination with one or more of the three principal references discussed above. Additional

references are also cited under the provisions of MPEP 2131.01 to explain features or details that are inherent in certain prior art disclosures. This section summarizes these additional references.

(i) RFC 793

Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Protocol Specification RFC 793 (Sept. 1981).

RFC 793 is a printed publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of RFC 793 is attached as Exhibit D-6.

(ii) 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, FL (Nov. 7-11, 1998).

Masys is a printed publication published more than one year before the '180 Patent's earliest effective priority date of Apr. 26, 2000 and is prior art under 35 U.S.C. § 102(b). Masys is attached as Exhibit D-9.

(iii) Martin

David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb. 21, 1998).

Martin is a publication that was publicly available more than one year before the '180 Patent's earliest effective date of April 26, 2000 and is prior art under 35 U.S.C. § 102(b). Martin was also published before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(a). A copy of Martin is attached as Exhibit D-4.

(iv) Rosenberry

Ward Rosenberry, David Kenney, and Gerry Fisher, UNDERSTANDING DCE (1993).

Rosenberry is a publication that was publicly available more than one year before the '180 Patent's earliest effective date of April 26, 2000 and is prior art under 35 U.S.C. § 102(b). Rosenberry was also published more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of Rosenberry is attached as Exhibit D-8.

(v) Schneier

Bruce Schneier, APPLIED CRYPTOGRAPHY (1996).

Schneier is a publication that was publicly available more than one year before the '180 Patent's earliest effective date of April 26, 2000 and is prior art under 35 U.S.C. § 102(b). Schneier was also published more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of Schneier is attached as Exhibit D-5.

(vi) RFC 1034

P. Mockapetris, "Domain Names – Concepts and Facilities," RFC 1034 (Nov. 1987).

RFC 1034 is a publication that was publicly available more than one year before the '151 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of RFC 1034 is attached as Exhibit D-10.

B. Statutory Bases for Proposed Rejections of the Claims

The following is a quotation of 35 U.S.C. § 102 that forms the basis for all of the following anticipation rejections:

A person shall be entitled to a patent unless ...

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, or

(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, or

(e) the invention was described in ... (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent....

The following is a quotation of 35 U.S.C. § 103(a) that forms the basis of all obviousness rejections:

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 negated by the manner in which the invention was made.

C. Proposed Rejections of the Claims

(a) Proposed Rejections Based on Lendenmann

Proposed Rejection #1. Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102, as shown by detailed explanation in the claim chart provided at Exhibit E-1, chart E-1.1.

Proposed Rejection #2. Claims 5, 21, and 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-1, chart E-1.2.

Proposed Rejection #3. Claims 7, 23, and 38 are obvious over Lendenmann in view of Martin under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-1, chart E-1.3.

Proposed Rejection #4. Claims 11, 27 and 41 are obvious over Lendenmann under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-1, chart E-1.4.

(b) Proposed Rejections Based on Kiuchi

Proposed Rejection #5. Claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102, as shown by detailed explanation in the claim chart provided at Exhibit E-2, chart E-2.1.

Proposed Rejection #6. Claims 3 and 19 are obvious over Kiuchi in view of Masys under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-2, chart E-2.2.

Proposed Rejection #7. Claims 7, 23 and 38 are obvious over Kiuchi in view of Martin under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-2, chart E-2.3.

Proposed Rejection #8. Claims 11, 27, and 41 are obvious over Kiuchi alone under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-2, chart E-2.4.

(c) Proposed Rejections Based on Solana

Proposed Rejection #9. Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102, as shown by detailed explanation in the claim chart provided at Exhibit E-3, chart E-3.1.

(d) Proposed Rejections Based on Schimpf and Rosenberry

Proposed Rejection #10. Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103, as shown by detailed explanation in the claim chart provided at Exhibit E-4, chart E-4.1.

D. Claim Interpretation

“During patent examination, the pending claims must be ‘given their broadest reasonable interpretation consistent with the specification.’” (MPEP § 2111). The standards of claim interpretation that must be used by the courts in patent litigation are different than the claim interpretation standard that must be used by the Office in claim examination proceedings (including reexamination). Therefore, any claim interpretations submitted herein for the purpose of demonstrating a substantial new question of patentability are neither binding upon the real parties in interest in any litigation related to the ’180 patent nor do such claim interpretations necessarily correspond to the construction of claims under the legal standards that are mandated to be used by the courts in litigation. (*See* MPEP at § 2686.04.II (determination of a substantial new question of patentability is made independently of court’s decision on validity because of different standards of proof and claim interpretation employed by the District Courts and the Office); *see also, In re Zletz*, 893 F.2d 319, 322, 13 USPQ2d 1320,1322 (Fed. Cir. 1989); 35 U.S.C. §305).

The ’180 patent was asserted in prior litigation, styled *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80 in the Eastern District of Texas. Various terms in the ’180 patent were construed by the district court. As potentially helpful guidance in giving the claims the broadest reasonable interpretation consistent with the specification, the district court’s Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009) is attached as Exhibit B-4.

V. List of Exhibits

- Exhibit A U.S. Patent 7,188,180
- Exhibit B-1 File History of U.S. Patent 7,188,180
- Exhibit B-2 File History of U.S. Patent Application No. 09/558,209
- Exhibit B-3 File History of Reexamination Control No. 95/001,270, reexamination of U.S. 7,188,180 requested by Microsoft Corp.
- Exhibit B-4 *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009).
- Exhibit C-1 U.S. Patent 6,502,135
- Exhibit C-2 U.S. Patent 7,010,604
- Exhibit C-3 Provisional Application 60/106,261
- Exhibit C-4 Provisional Application 60/137,704
- Exhibit D-1 “Lendenmann”: Rolf Lendenmann, UNDERSTANDING OSF DCE 1.1 FOR AIX AND OS/2, IBM International Technical Support Organization (Oct. 1995).
- Exhibit D-2 “Kiuchi”: Takahiro Kiuchi and Shigekoto Kaihara, “C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet,” published in the Proceedings of SNDSS 1996.
- Exhibit D-3 “Solana”: Eduardo Solana and Jürgen Harms, “Flexible Internet Secure Transactions Based on Collaborative Domains,” Security Protocols Workshop 1997, pp. 37-51.
- Exhibit D-4 “Martin”: David M. Martin, “A Framework for Local Anonymity in the Internet,” Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).
- Exhibit D-5 “Schneier”: Bruce Schneier, APPLIED CRYPTOGRAPHY (1996).
- Exhibit D-6 “RFC 793”: Information Sciences Institute, “Transmission Control Protocol,” DARPA Internet Program Protocol Specification RFC 793 (Sept. 1981).
- Exhibit D-7 “Schimpf”: Brian C. Schimpf, “Securing Web Access with DCE,” presented at Network and Distributed System Security (Feb. 10-11, 1997).
- Exhibit D-8 “Rosenberry”: Ward Rosenberry, David Kenney, and Gerry Fisher, UNDERSTANDING DCE (1993).

Request for *Inter partes* Reexamination
U.S. Patent No. 7,188,180

- Exhibit D-9 “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, FL (Nov. 7-11, 1998).
- Exhibit D-10 “RFC 1034”: “Domain Names – Concepts and Facilities,” RFC 1034 (Nov. 1987).
- Exhibit E-1 Claim charts applying Lendenmann as a primary reference to the '180 patent.
- Exhibit E-2 Claim charts applying Kiuchi as a primary reference to the '180 patent.
- Exhibit E-3 Claim charts applying Solana as a primary reference to the '180 patent.
- Exhibit E-4 Claim charts applying Schimpf and Rosenberry as references to the '180 patent.

VI. Conclusion

For the reasons set forth above, the Requester has established a reasonable likelihood that the Requester will prevail with respect to claims 1-41 of the '180 patent. The analysis of the claims in this request demonstrates the invalidity of these claims in view of the prior art not previously considered by the Patent Office. Therefore, the Requester asks that this request for reexamination be granted and that all of claims 1-41 be canceled.

As identified in the attached Certificate of Service and in accordance with 37 C.F.R. §§ 1.33(c) and 1.915(b)(6), a copy of the present request, in its entirety, is being served to the address of the attorney or agent of record.

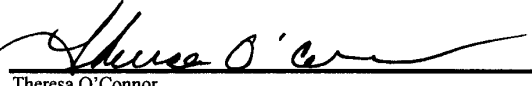
Please direct all correspondence in this matter to the undersigned.

Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: October 25, 2011
HAYNES AND BOONE, LLP
Customer No. 27683
Telephone: 214/651-5533
Facsimile: 214/200-0808
Attorney Docket No.: 43614.100

CERTIFICATE OF SERVICE
I hereby certify that this correspondence, all attachments, and any corresponding filing fee is being transmitted via the Electronic Filing System (EFS) Web with the United States Patent and Trademark Office on <u>October 25, 2011</u> .

Theresa O'Connor

VII. Certificate of Service

The undersigned certifies that copies of the following,

- (1) Request for *Inter Partes* Reexamination Transmittal Form;
- (2) PTO 1449 Modified Form;
- (3) Request for *Inter Partes* Reexamination; and
- (4) Exhibits A through E-4

in their entirety were served on:

McDermott Will & Emery
600 13th Street, NW
Washington DC 20005-3096

the attorney of record for the assignee of U.S. Patent No. 7,188,180, in accordance with 37 C.F.R. § 1.915 (b)(6), on the 25th day of October, 2011.

/David L. McCombs/
David L. McCombs, Registration No. 32,271

Exhibit A

U.S. Patent 7,188,180

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853



US007188180B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.:** **US 7,188,180 B2**

(45) **Date of Patent:** **Mar. 6, 2007**

(54) **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Durham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VimetX, 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 413 days.

(21) Appl. No.: **10/702,486**

(22) Filed: **Nov. 7, 2003**

(65) **Prior Publication Data**

US 2004/0107285 A1 Jun. 3, 2004

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. 60/137,704, filed on Jun. 7, 1999, provisional application No. 60/106,261, filed on Oct. 30, 1998.

(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

4,933,846 A 6/1990 Humphrey et al.
5,341,426 A 8/1994 Barney et al.
5,588,060 A 12/1996 Aziz
5,689,566 A 11/1997 Nguyen

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Jun. 18, 2002), International Application No. PCT/US01/13260.

(Continued)

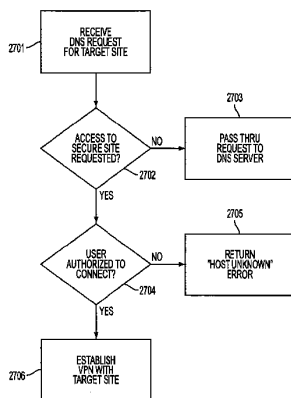
Primary Examiner—Krisna Lim

(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(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.

41 Claims, 40 Drawing Sheets



U.S. PATENT DOCUMENTS

5,787,172	A	7/1998	Arnold	
5,796,942	A	8/1998	Esbensen	
5,805,801	A	9/1998	Holloway et al.	
5,842,040	A	11/1998	Hughes et al.	
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, Jr. et al.	
5,905,859	A	5/1999	Holloway et al.	
6,006,259	A	12/1999	Adelman et al.	
6,016,318	A	1/2000	Tomoiike	
6,052,788	A	4/2000	Wesinger, Jr. et al.	
6,079,020	A	6/2000	Liu	
6,092,200	A	7/2000	Muniyappa et al.	
6,119,171	A *	9/2000	Alkhatib	709/245
6,119,234	A *	9/2000	Aziz et al.	726/11
6,158,011	A	12/2000	Chen et al.	
6,178,409	B1	1/2001	Weber et al.	
6,178,505	B1	1/2001	Schneider et al.	
6,226,751	B1	5/2001	Arrow et al.	
6,243,749	B1	6/2001	Sitaraman et al.	
6,256,671	B1 *	7/2001	Strentzsch et al.	709/227
6,286,047	B1	9/2001	Ramanathan et al.	
6,330,562	B1	12/2001	Boden et al.	
6,332,158	B1	12/2001	Risley et al.	
6,353,614	B1	3/2002	Borella et al.	

FOREIGN PATENT DOCUMENTS

EP	0 814 589	12/1997
EP	0 814 589 A	12/1997
EP	0 838 930	4/1998
EP	0 838 930 A	4/1998
EP	0 858 189	8/1998
GB	2 317 792	4/1998
GB	2 317 792 A	4/1998
GB	2 334 181 A	8/1999
WO	9827783 A	6/1998
WO	WO 98/27783	6/1998
WO	WO 98 55930	12/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Search Report (dated Jun. 28, 2002), International Application No. PCT/US01/13261.
 Donald E. Eastlake, "Domain Name System Security Extensions", DNS Security Working Group, Apr. 1998, 51 pages.
 D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-297 and pp. 351-375.
 P. Srisuresh et al., "DNS extensions to Network Address Translators", Jul. 1998, 27 pages.
 Laurie Wells, "Security Icon", Oct. 19, 1998, 1 page.
 W. Stallings, "Cryptography And Network Security", 2nd Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.

W. Stallings, "New Cryptography and Network Security Book", Jun. 8, 1998, 3 pages.
 Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication, 1996, pp. 963-967.
 Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.
 Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.
 Shree Murthy et al., "Congestion-Oriented Shortest Multipath Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.
 Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.
 James E. Bellaire, "New Statement of Rules—Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.
 D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.
 August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.
 Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.
 Linux FreeS/WAN Index File, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/on Feb. 21, 2002, 3 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.
 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.
 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.
 Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.
 F. Halsall, "Data Communications, Computer Networks And Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.
 Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transmission", pp. 1-23.
 Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.
 Rubin, Aviel D., Greer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.
 Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.
 Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606.
 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: <http://www.springerlink.com/content/4uac0tb0hecoma89/fulltext.pdf> (Abstract).

* cited by examiner

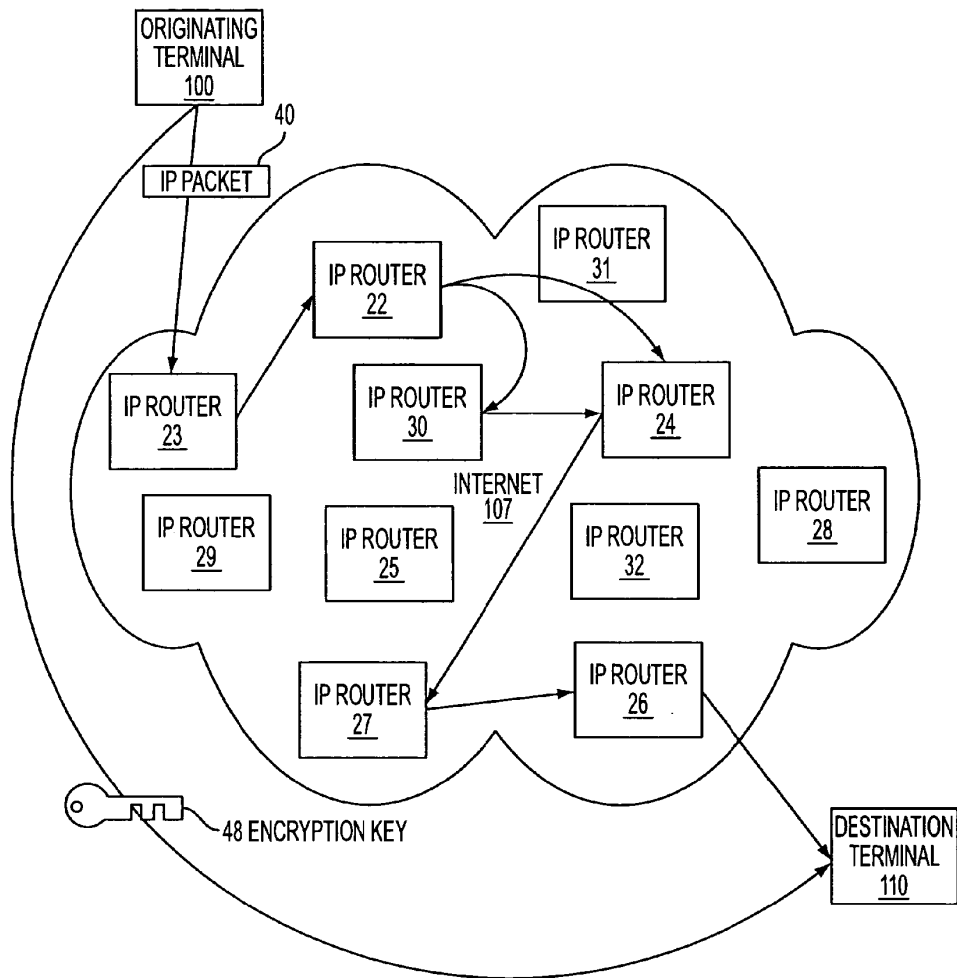


FIG. 1

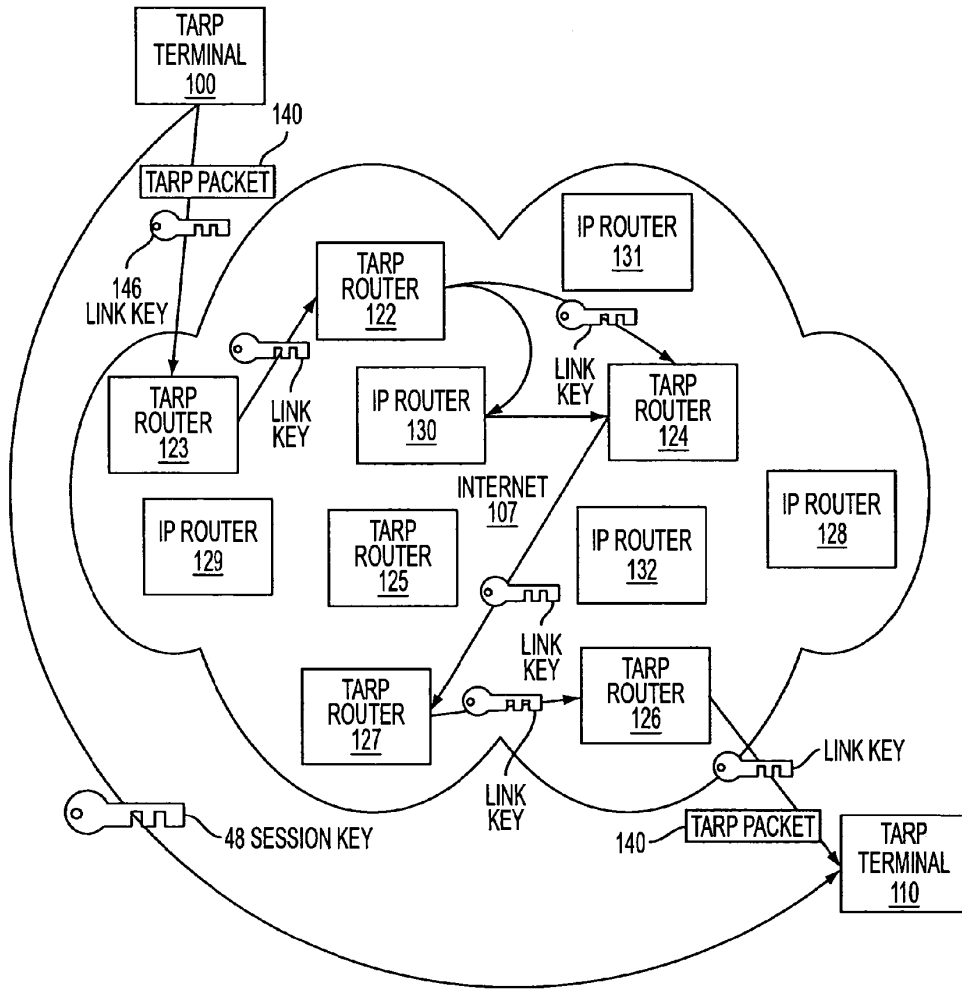


FIG. 2

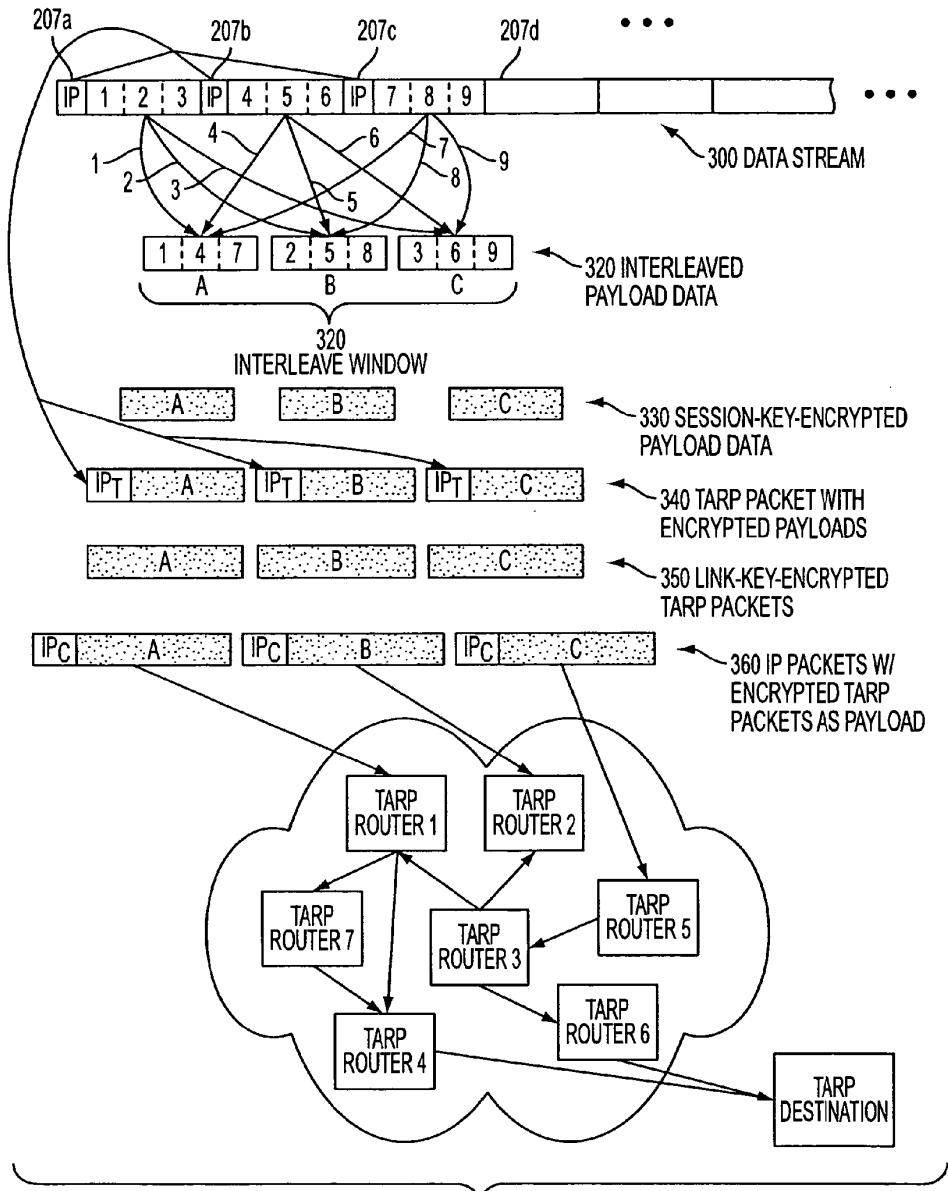


FIG. 3A

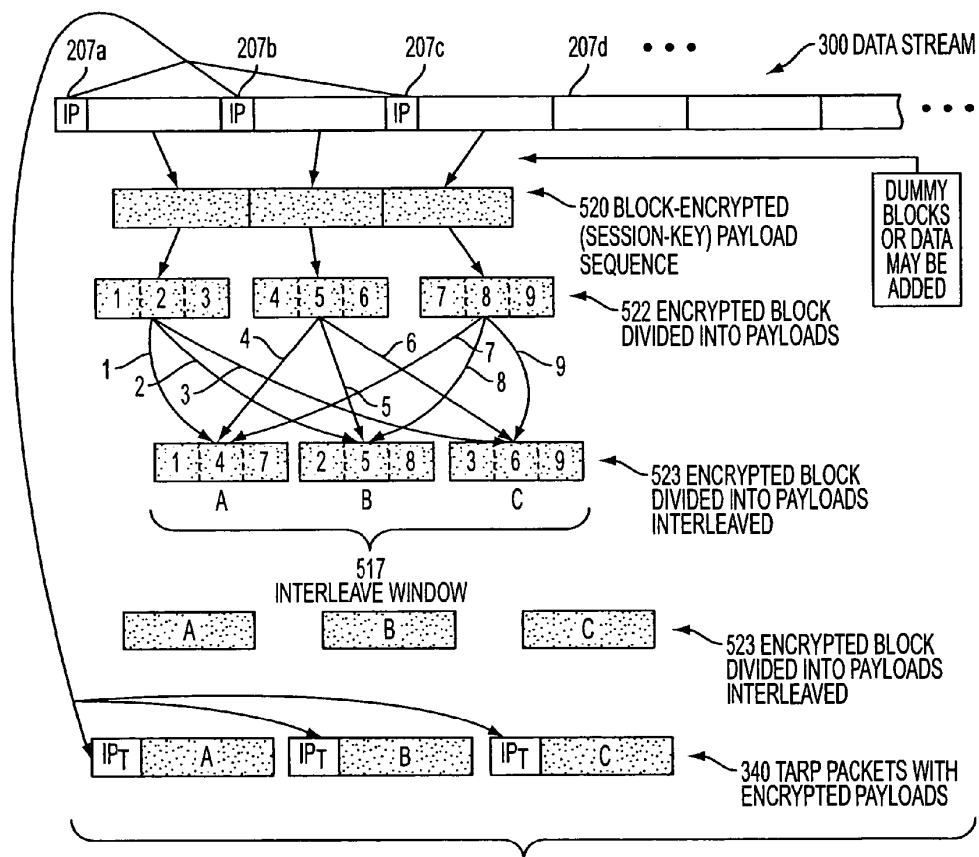


FIG. 3B

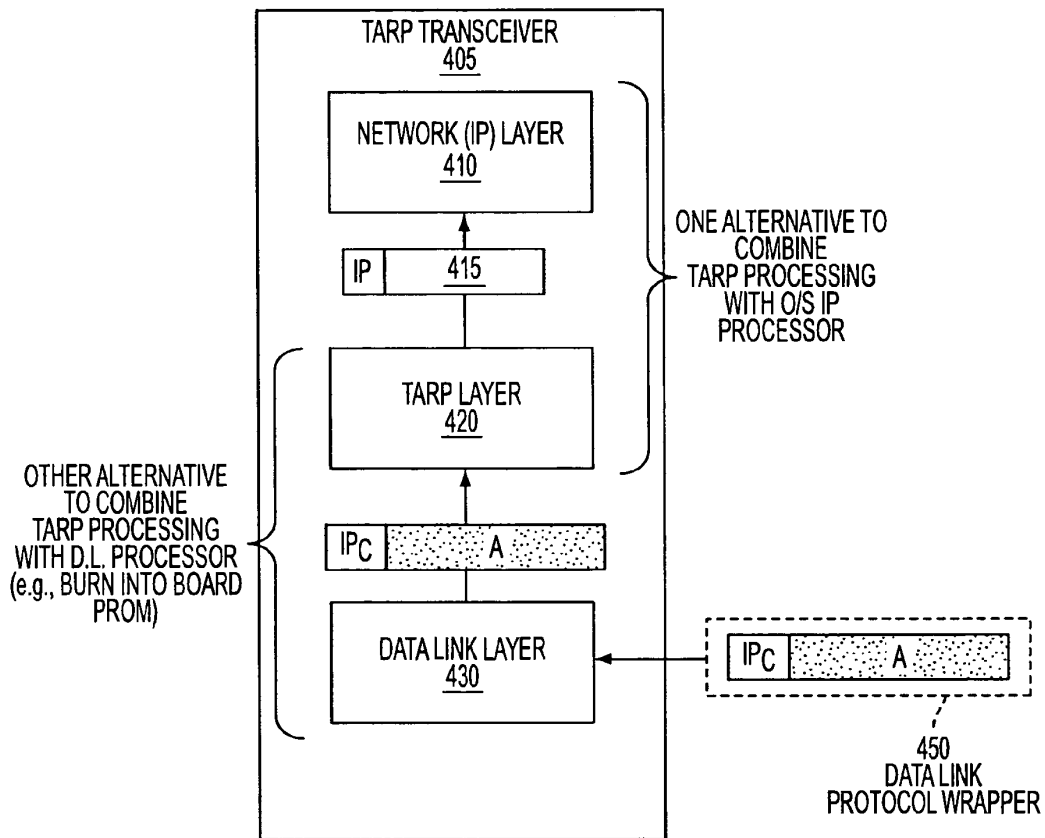


FIG. 4

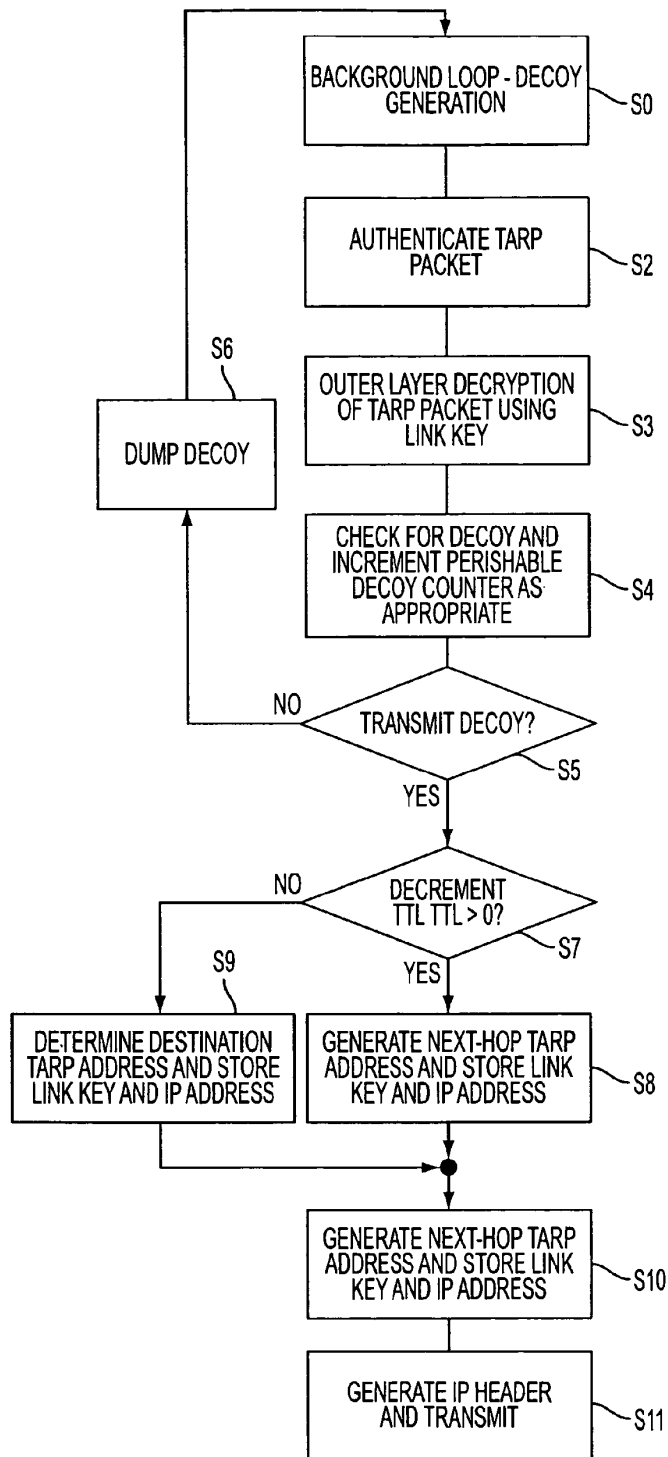


FIG. 5

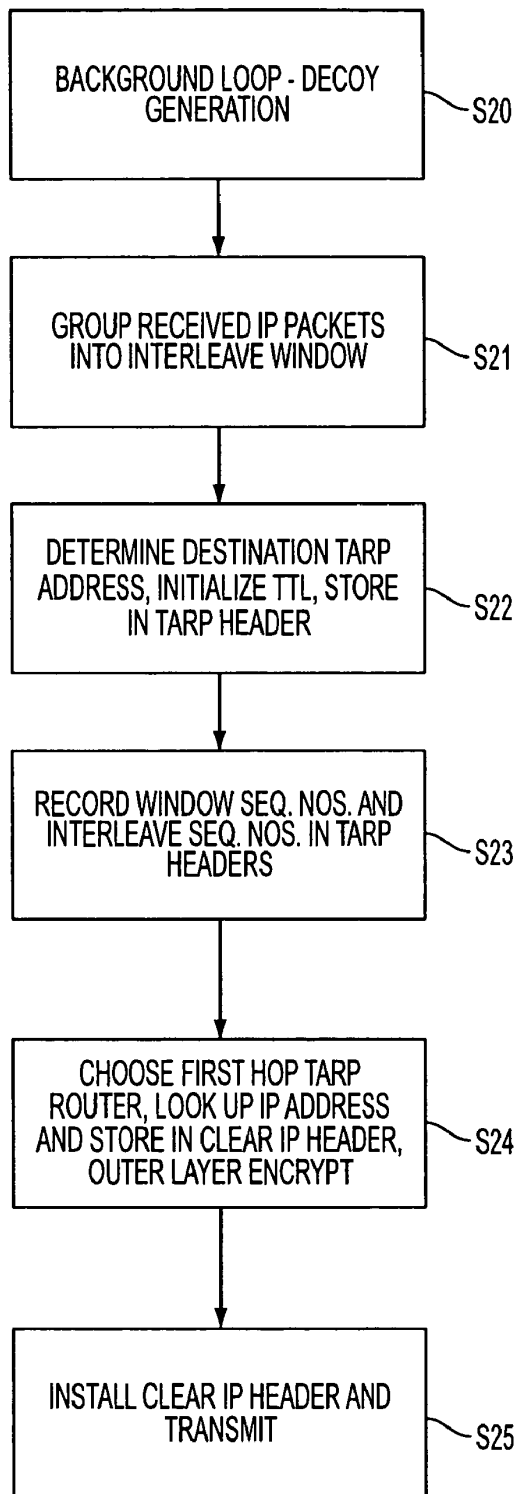


FIG. 6

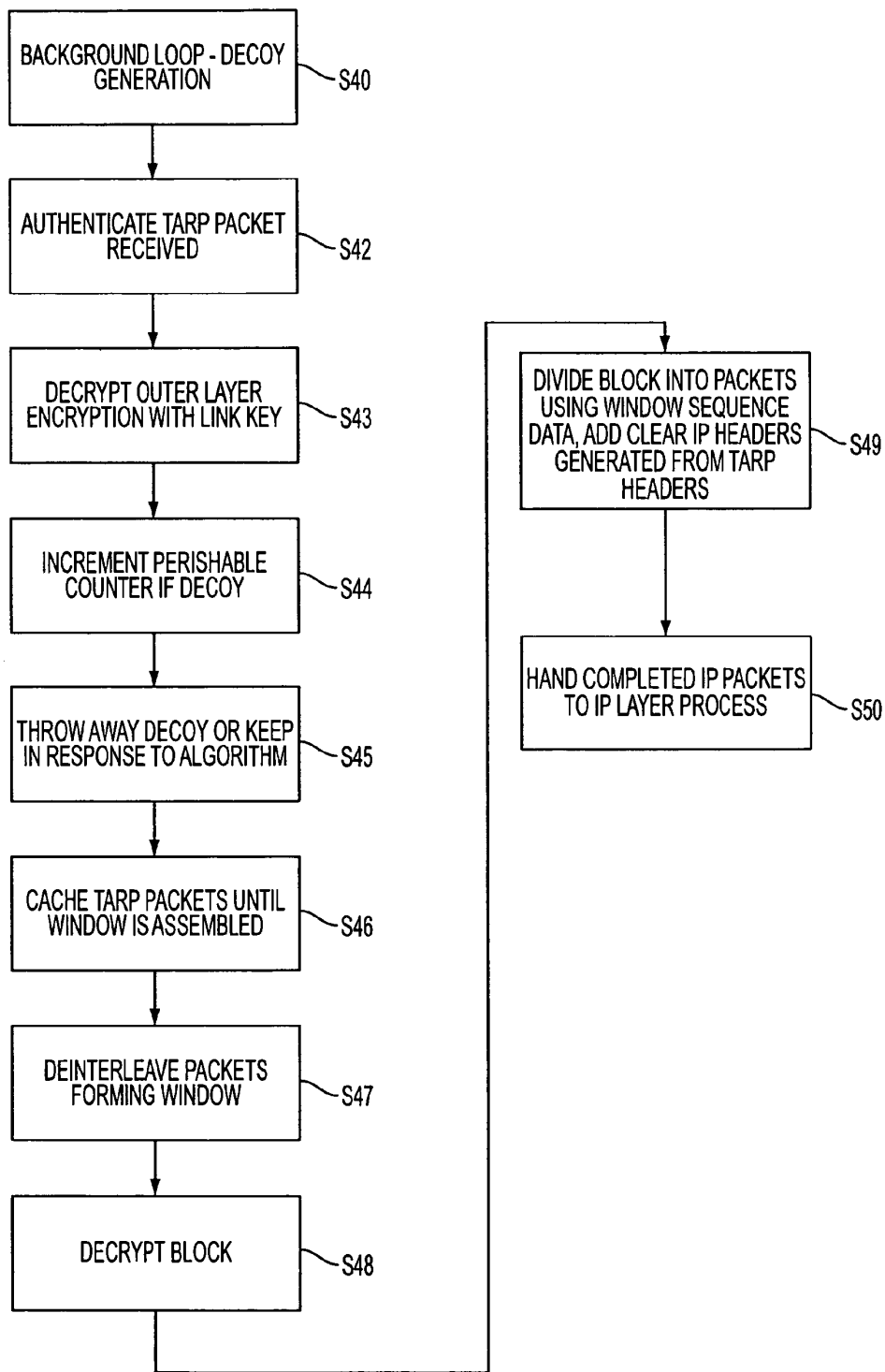


FIG. 7

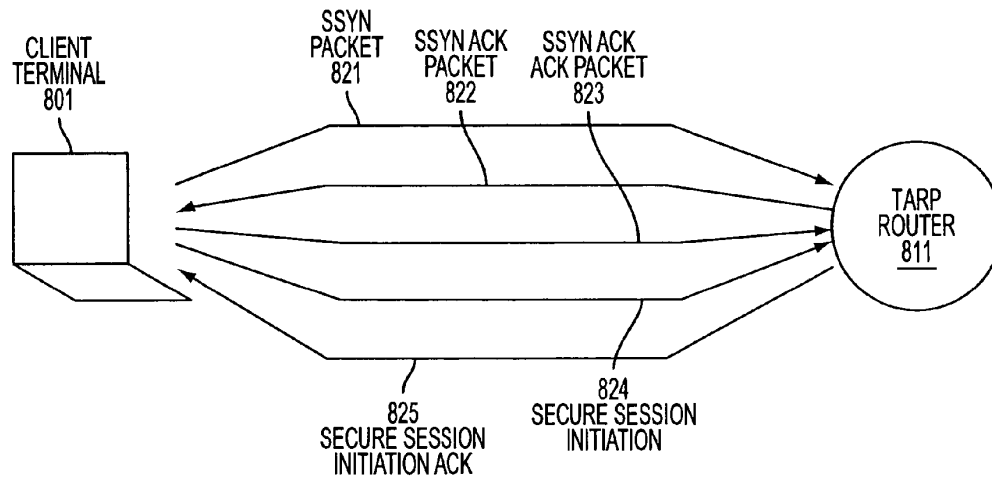


FIG. 8

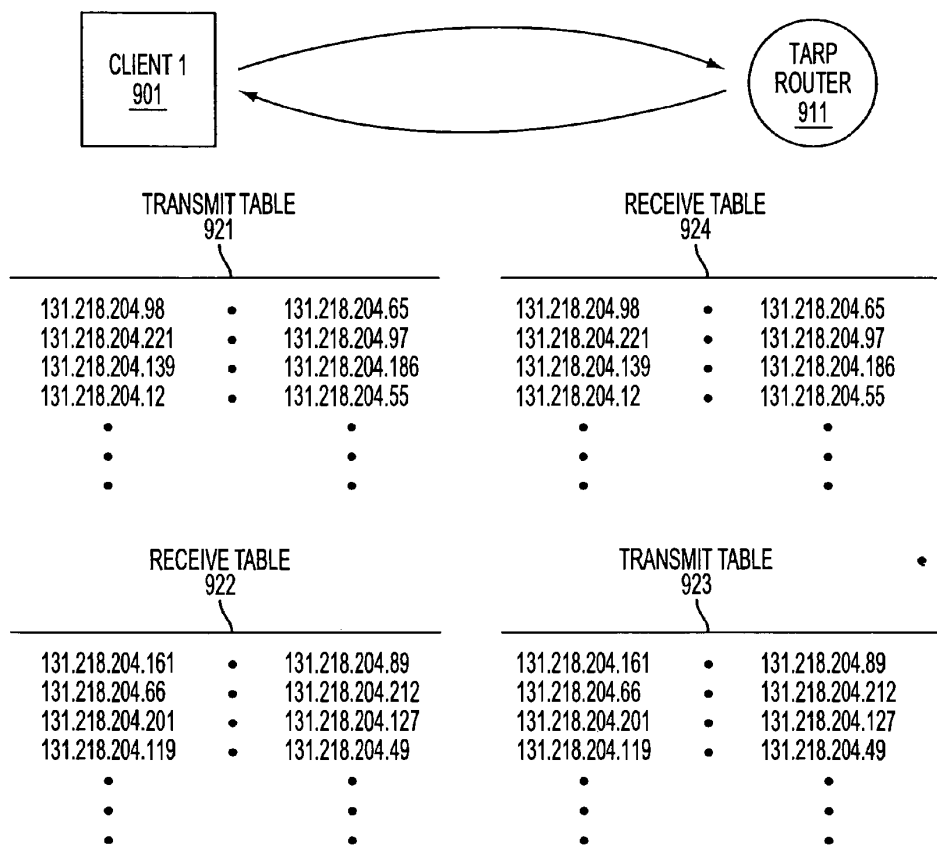


FIG. 9

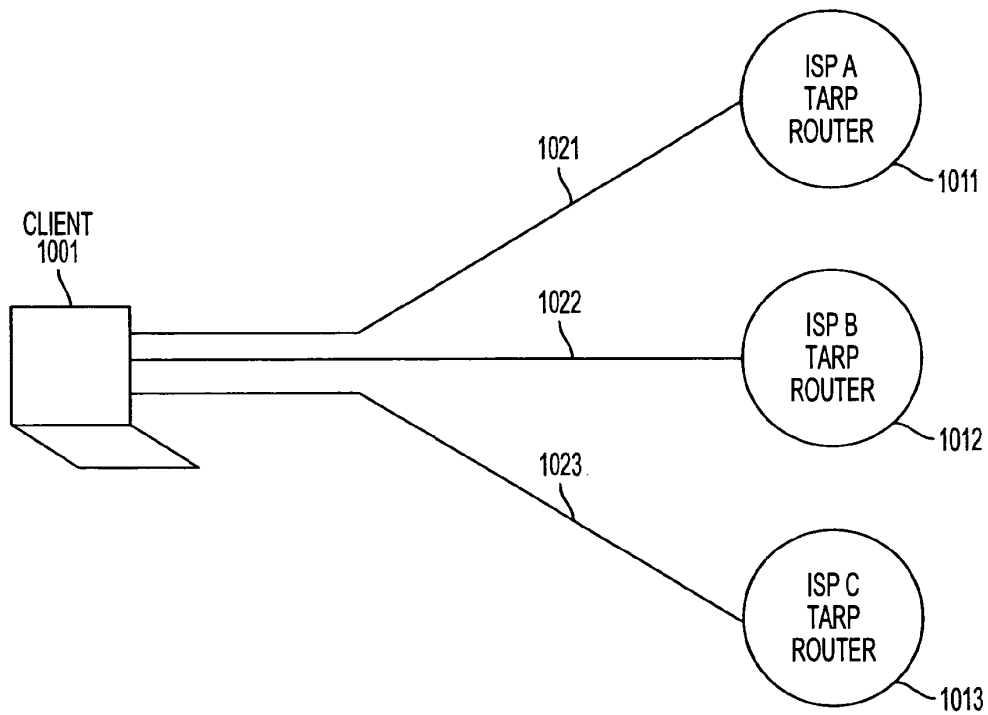


FIG. 10

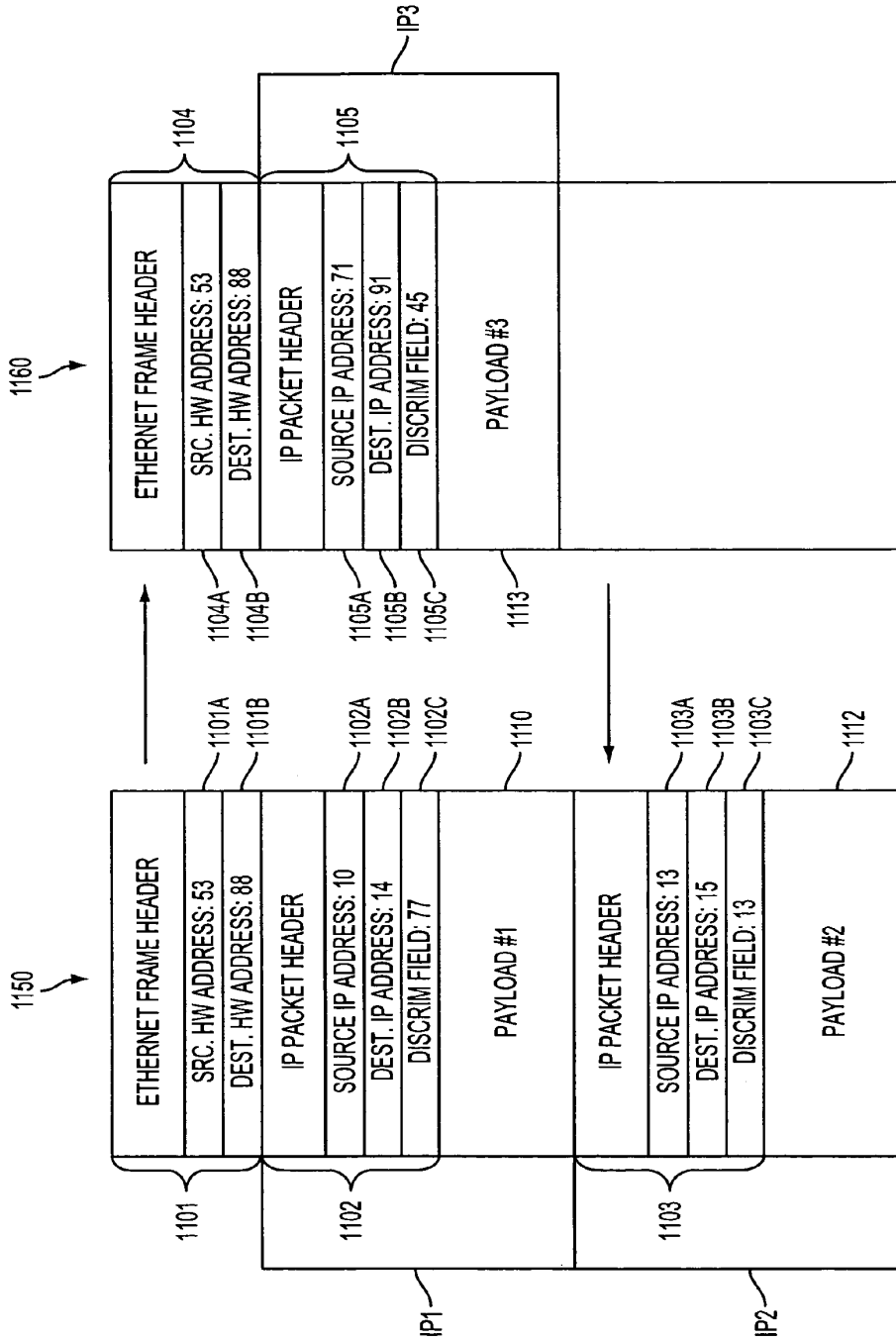


FIG. 11

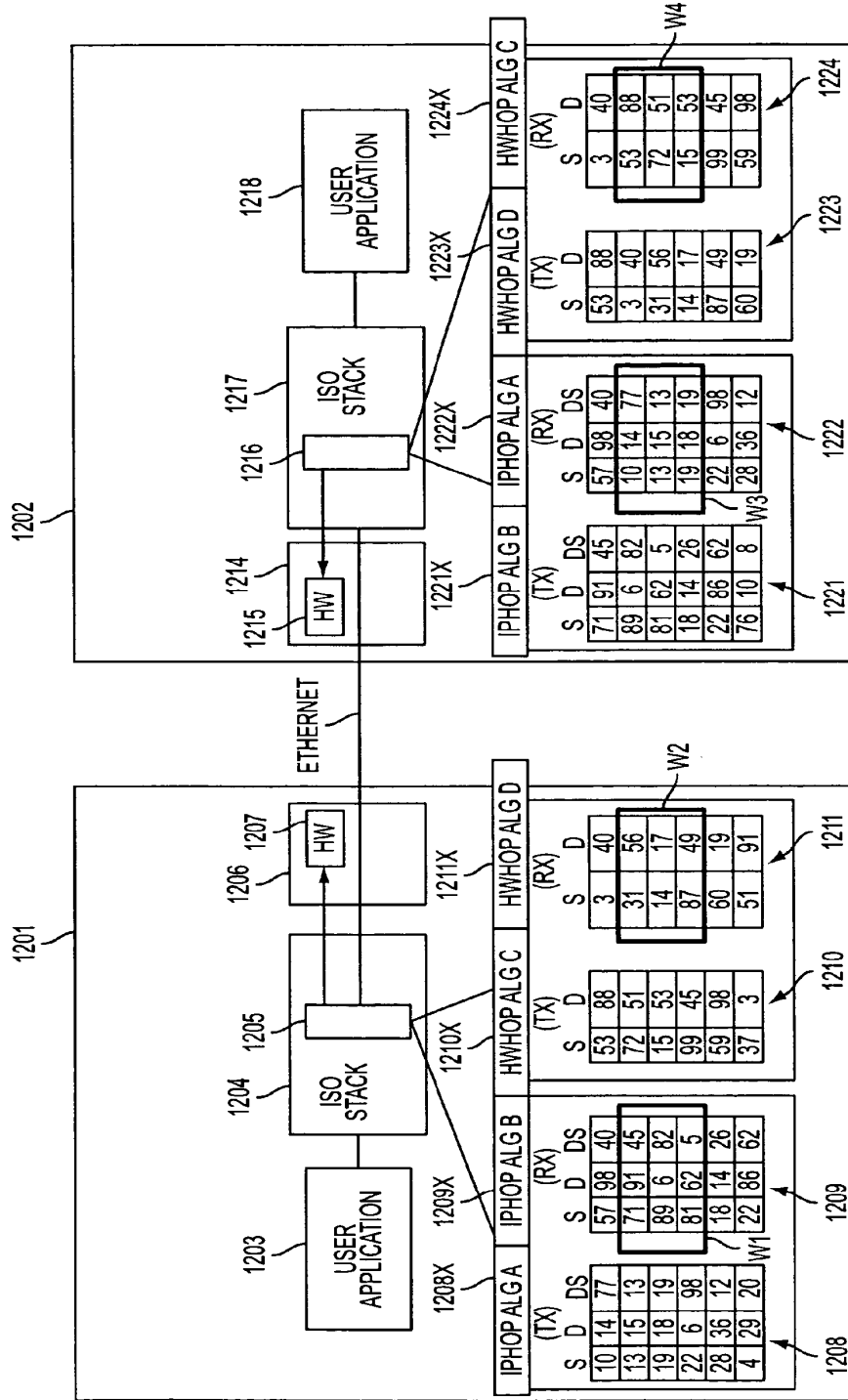


FIG. 12A

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

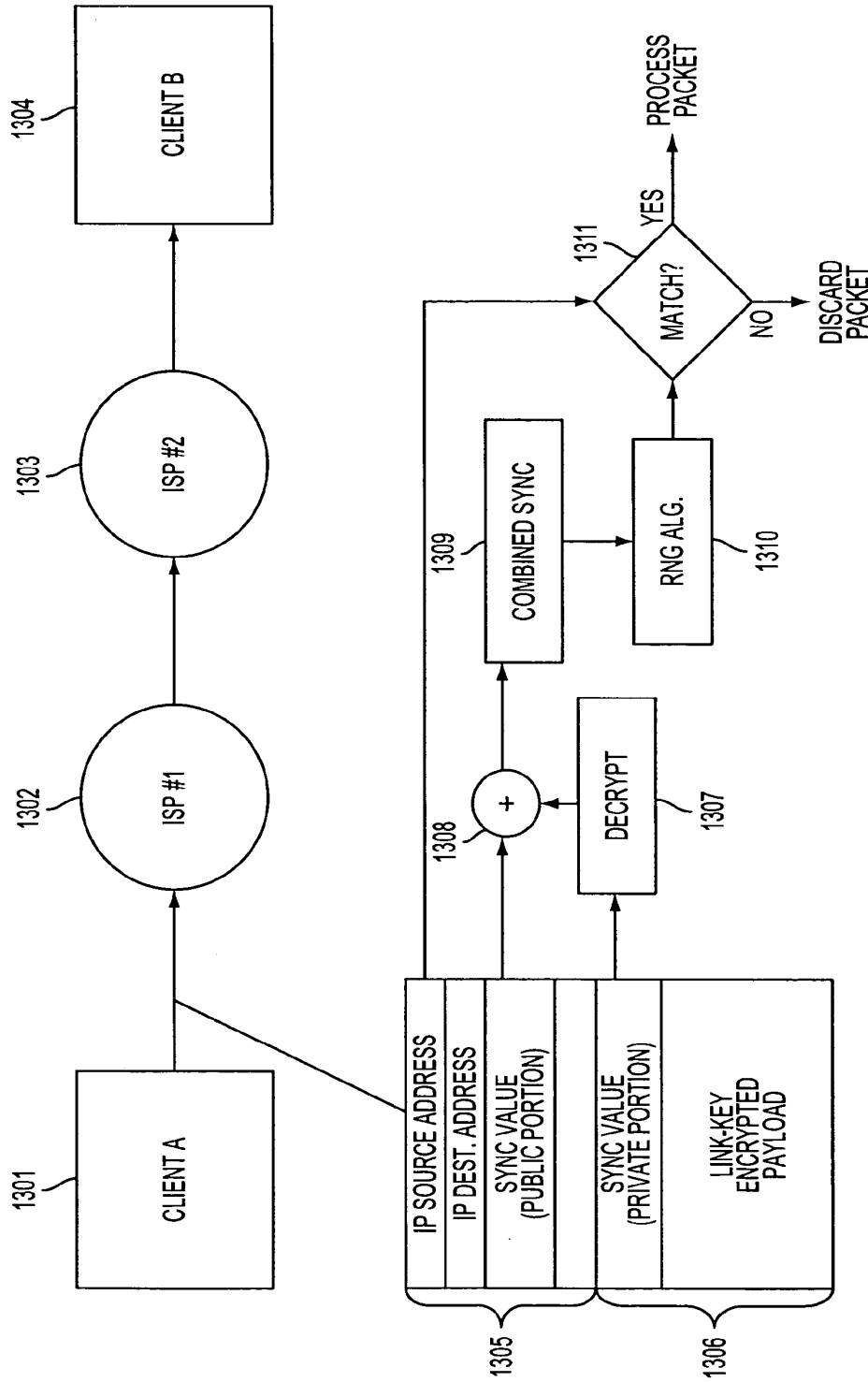


FIG. 13

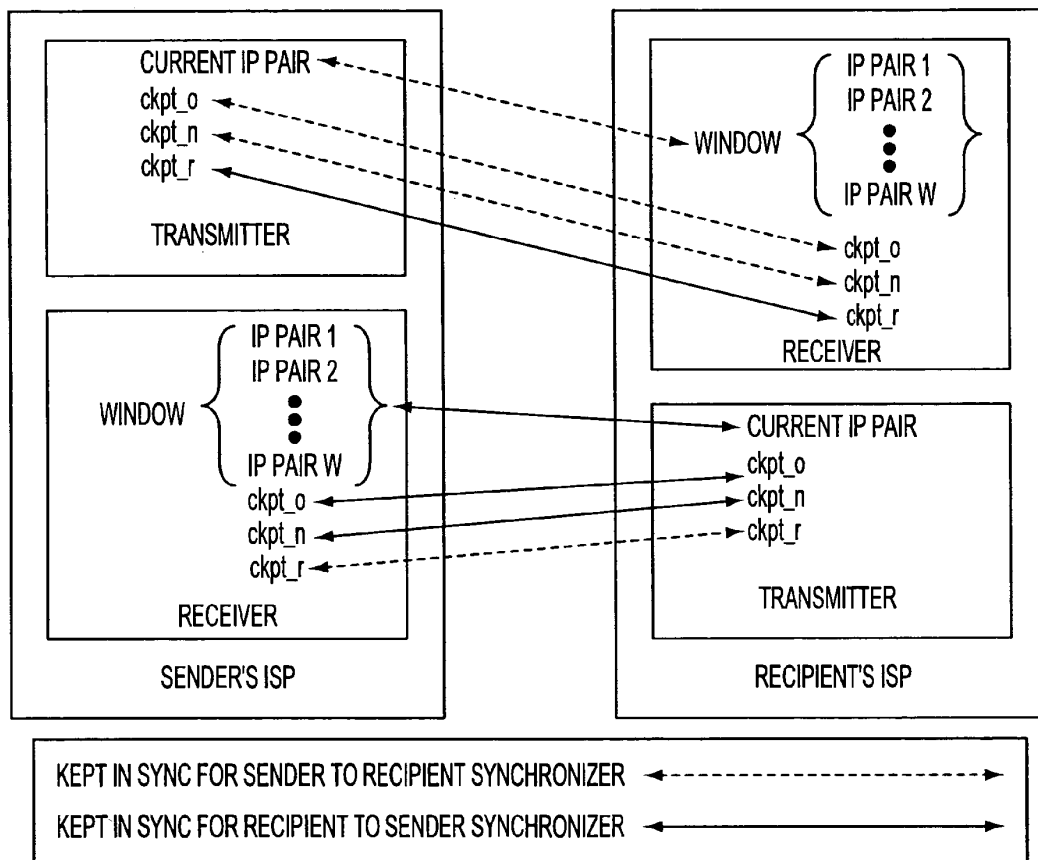


FIG. 14

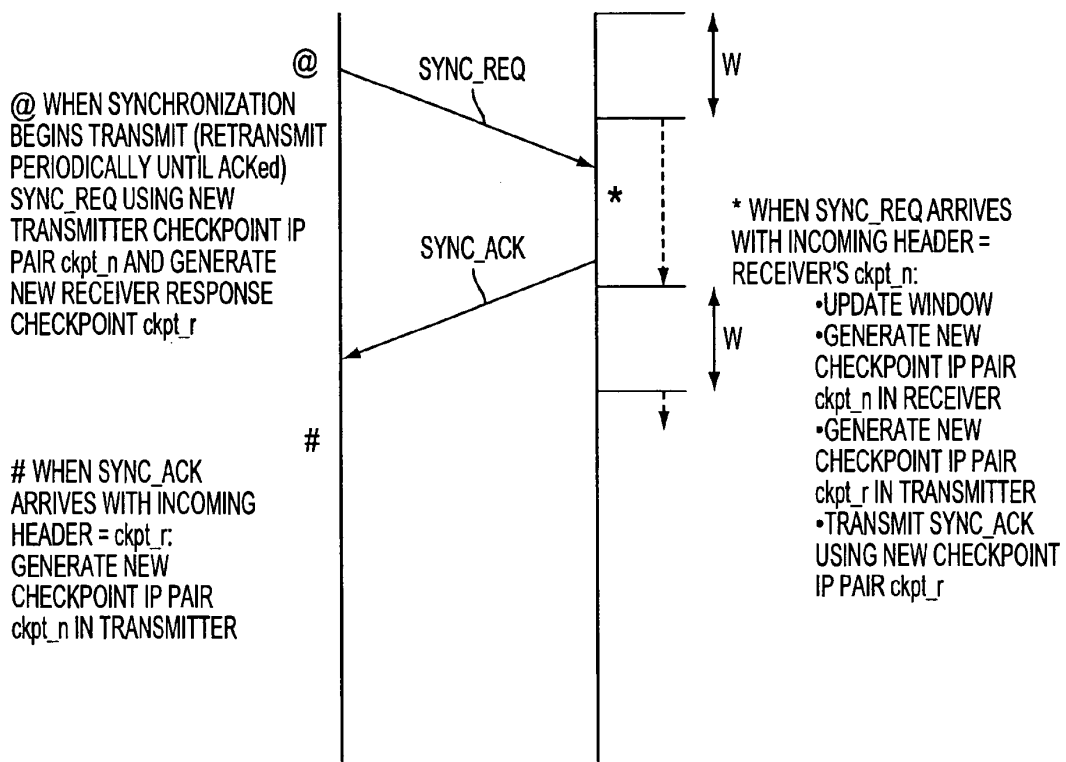


FIG. 15

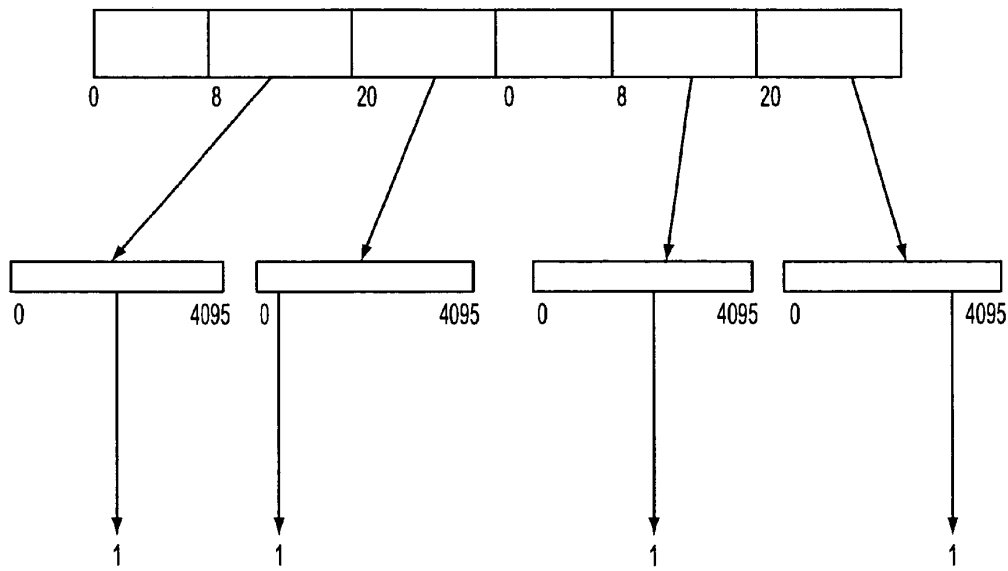


FIG. 16

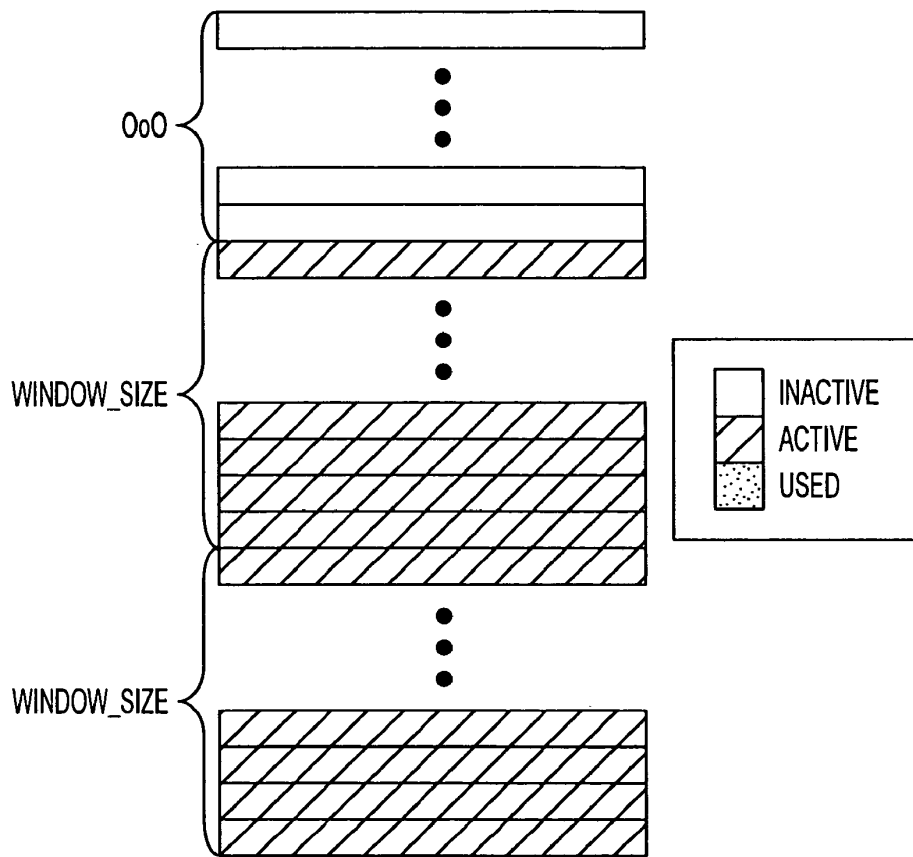


FIG. 17

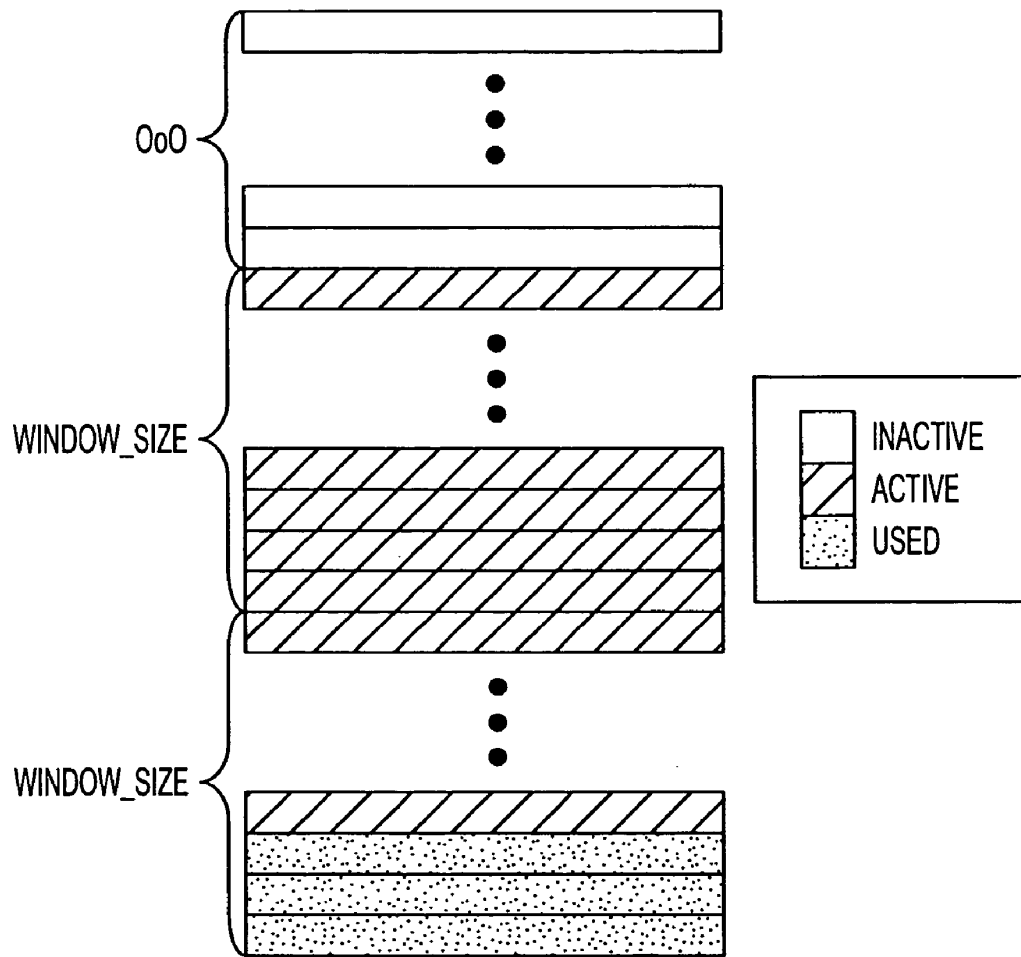


FIG. 18

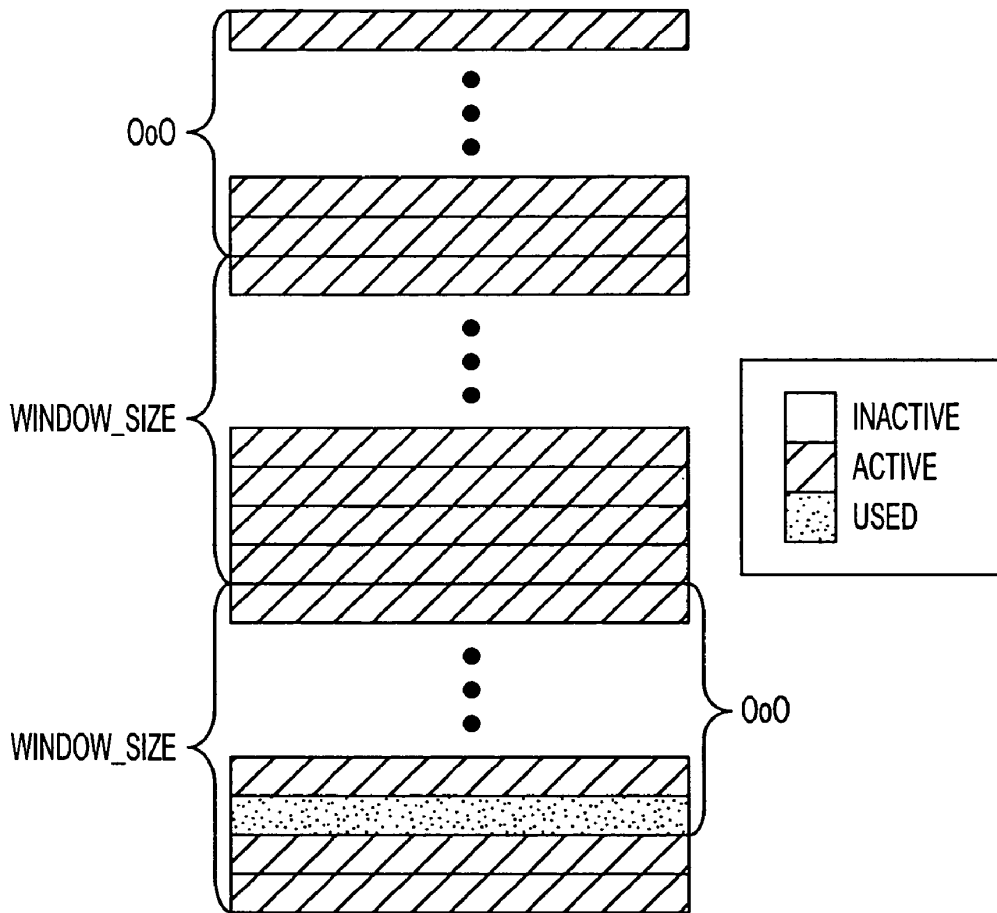


FIG. 19

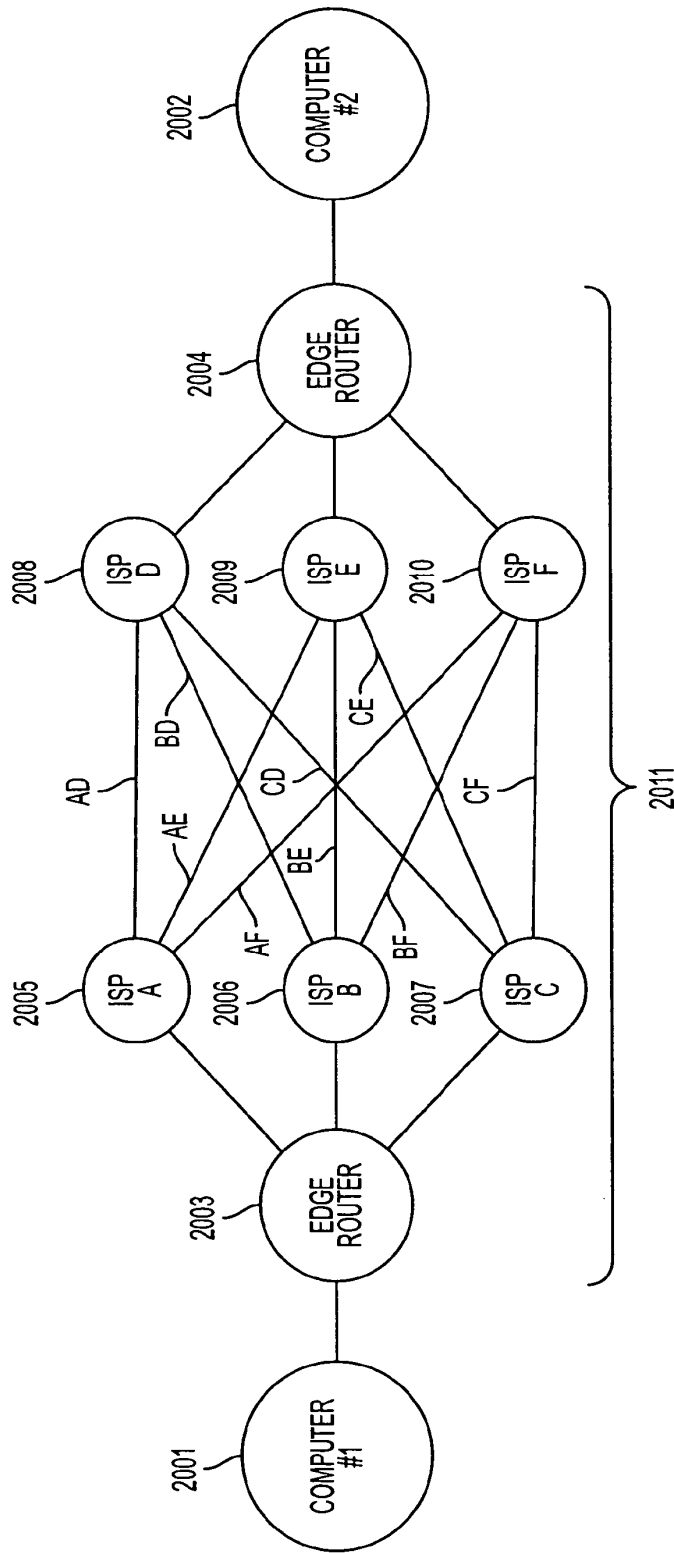


FIG. 20

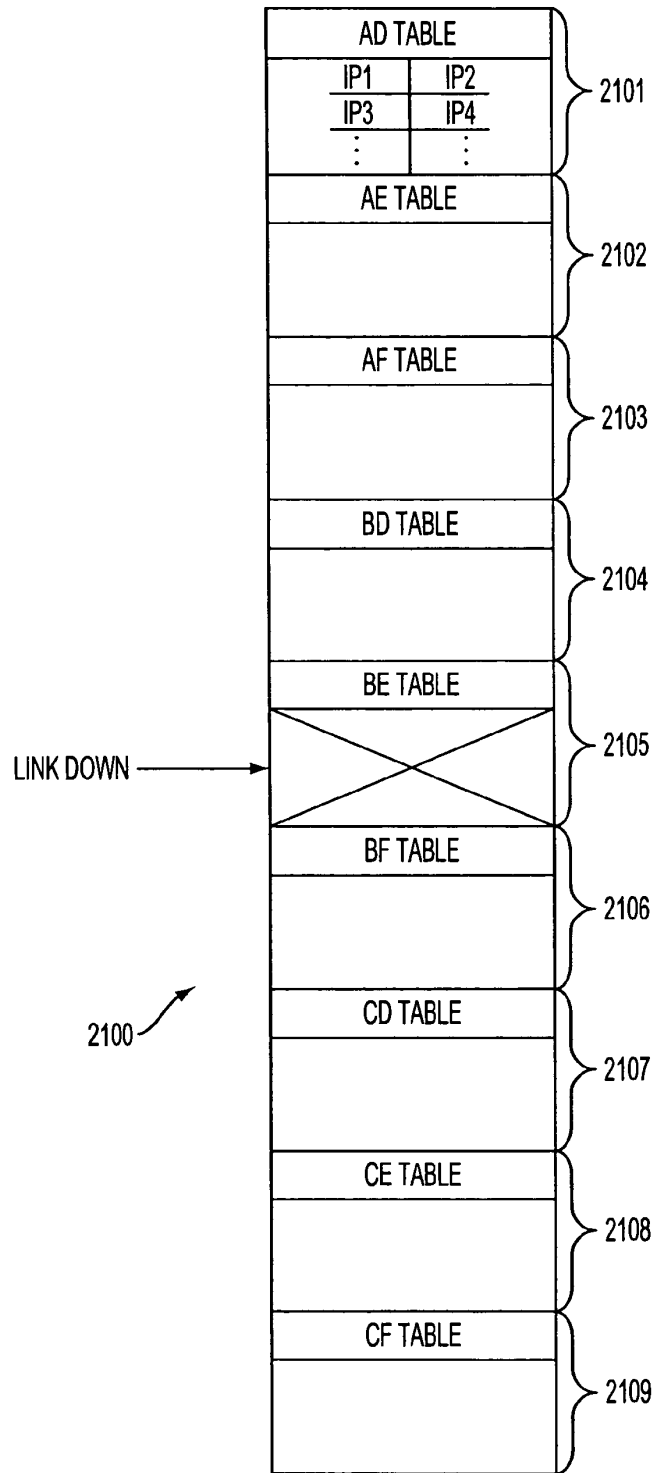


FIG. 21

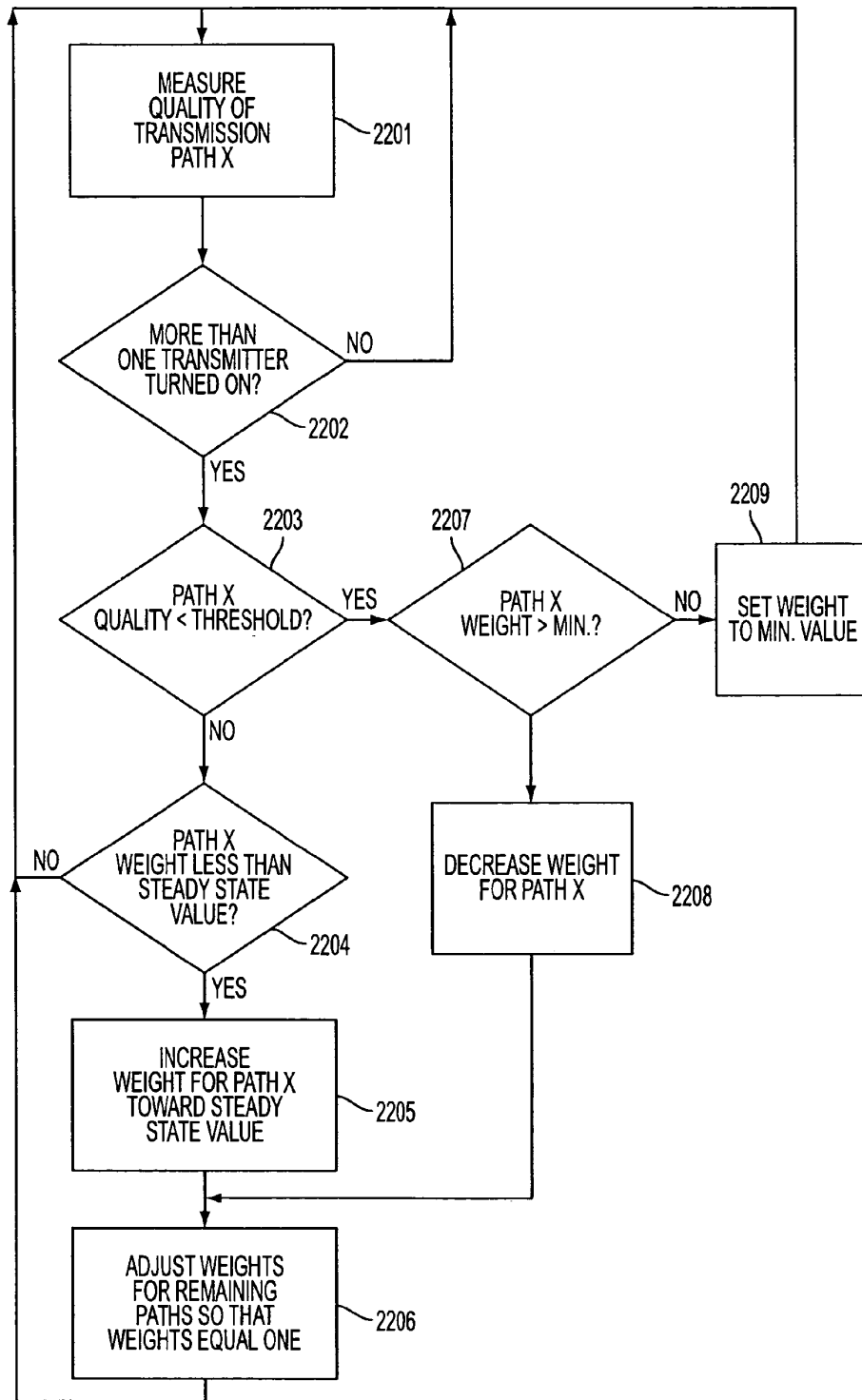


FIG. 22A

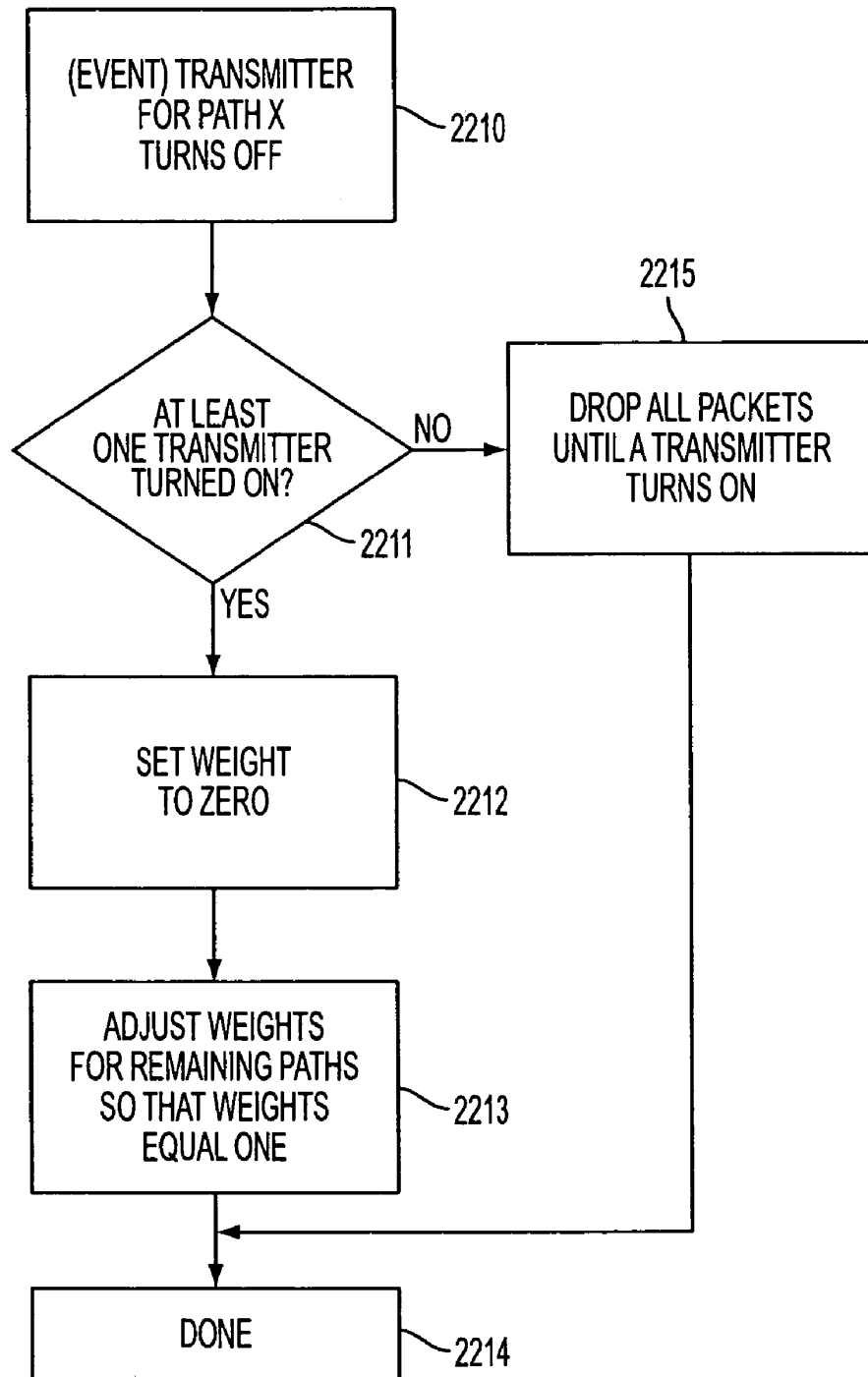


FIG. 22B

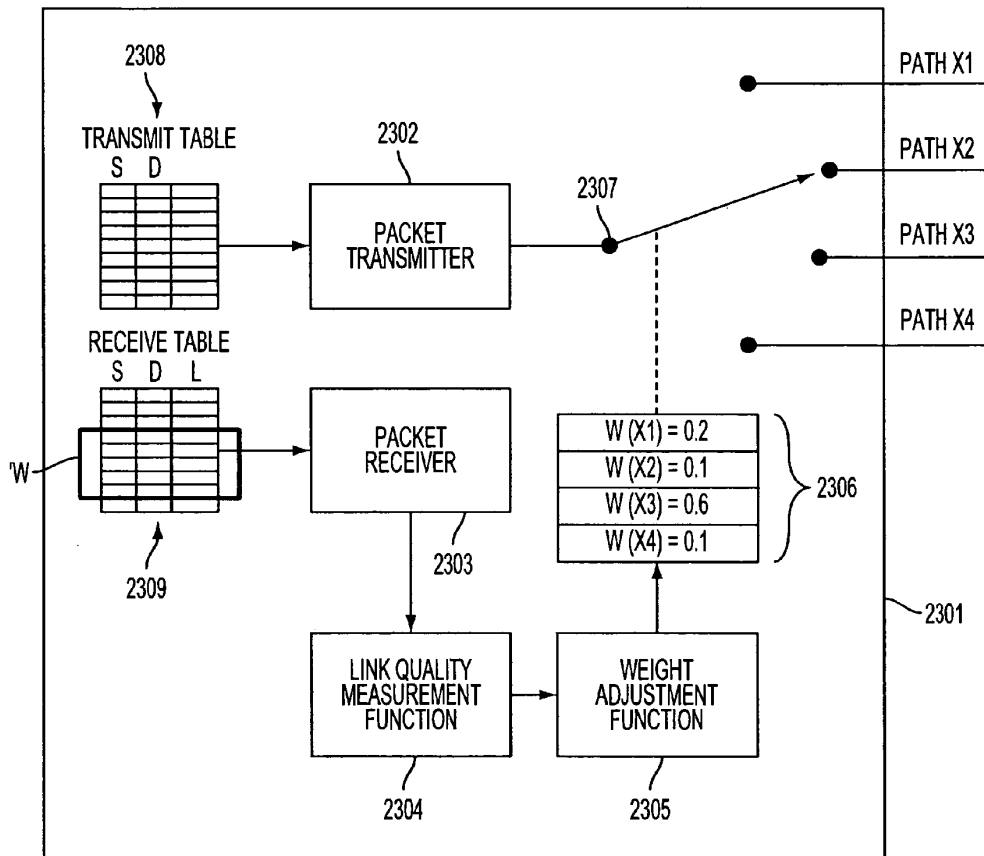


FIG. 23

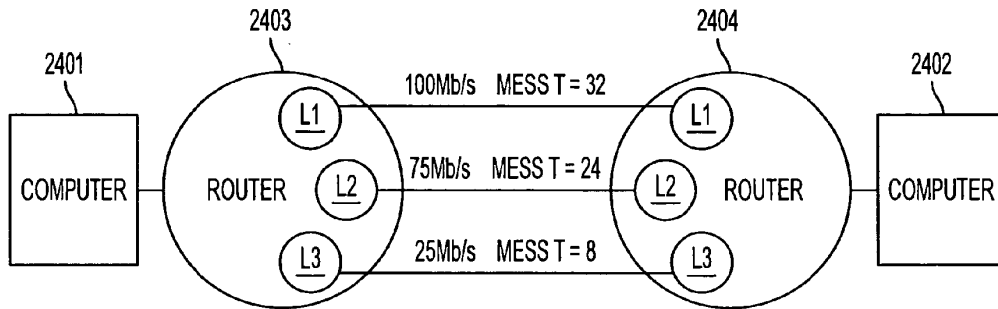


FIG. 24

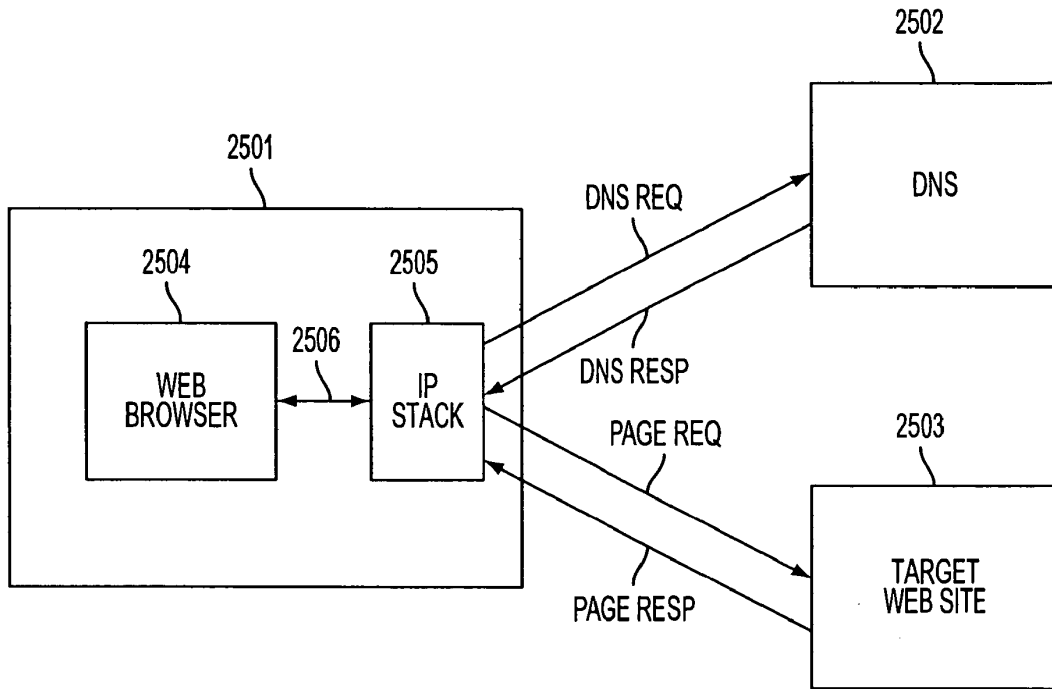


FIG. 25
(PRIOR ART)

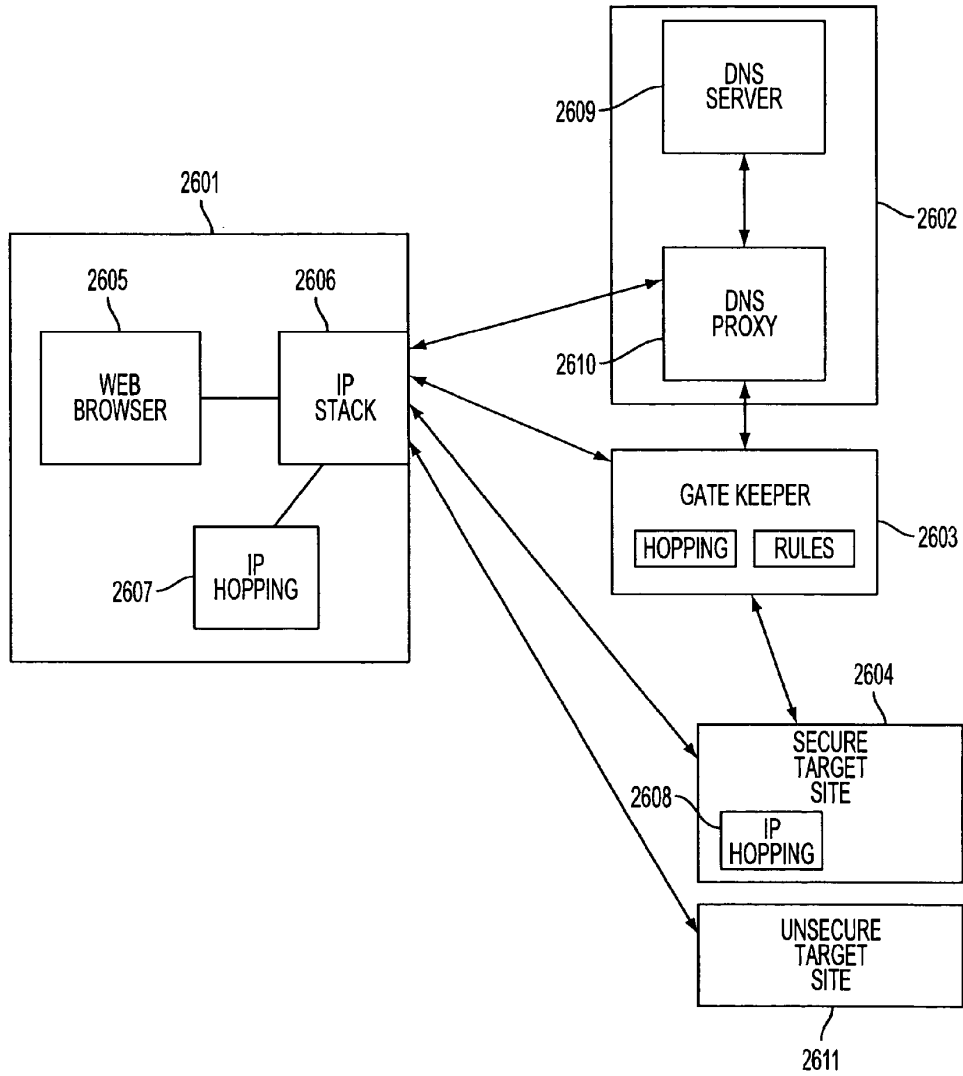


FIG. 26

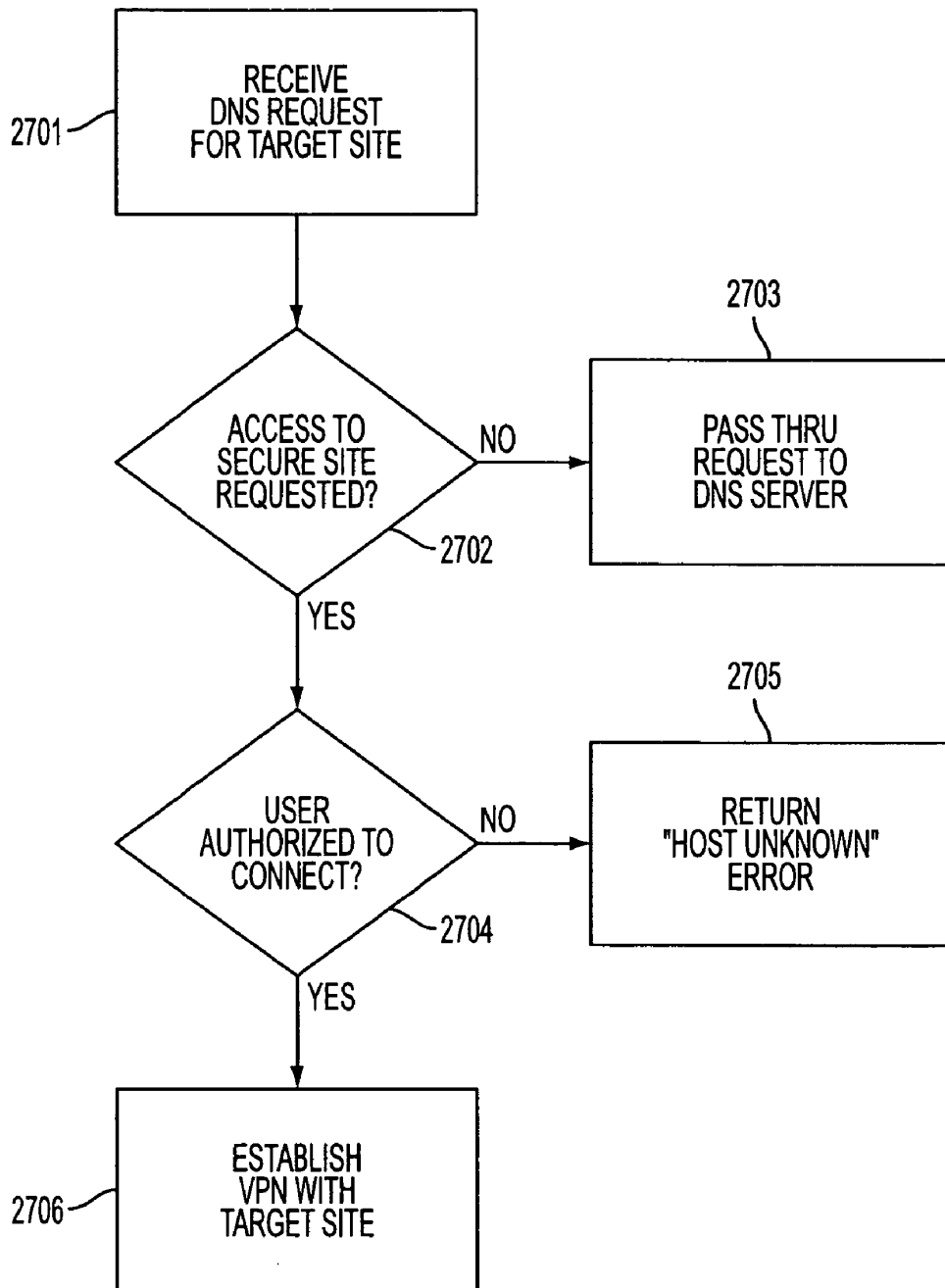


FIG. 27

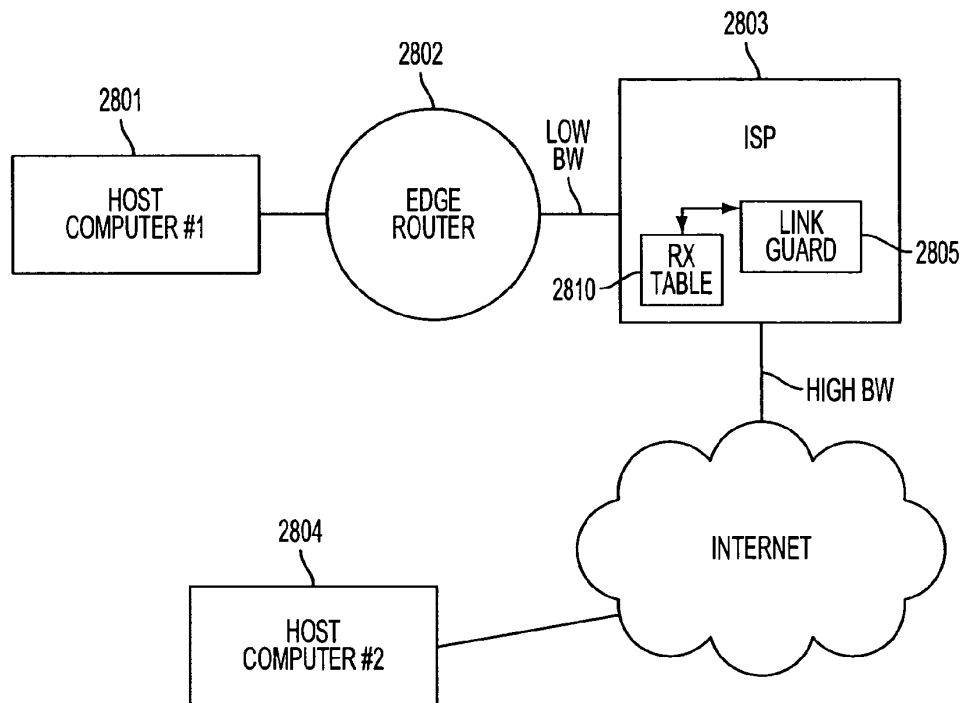


FIG. 28

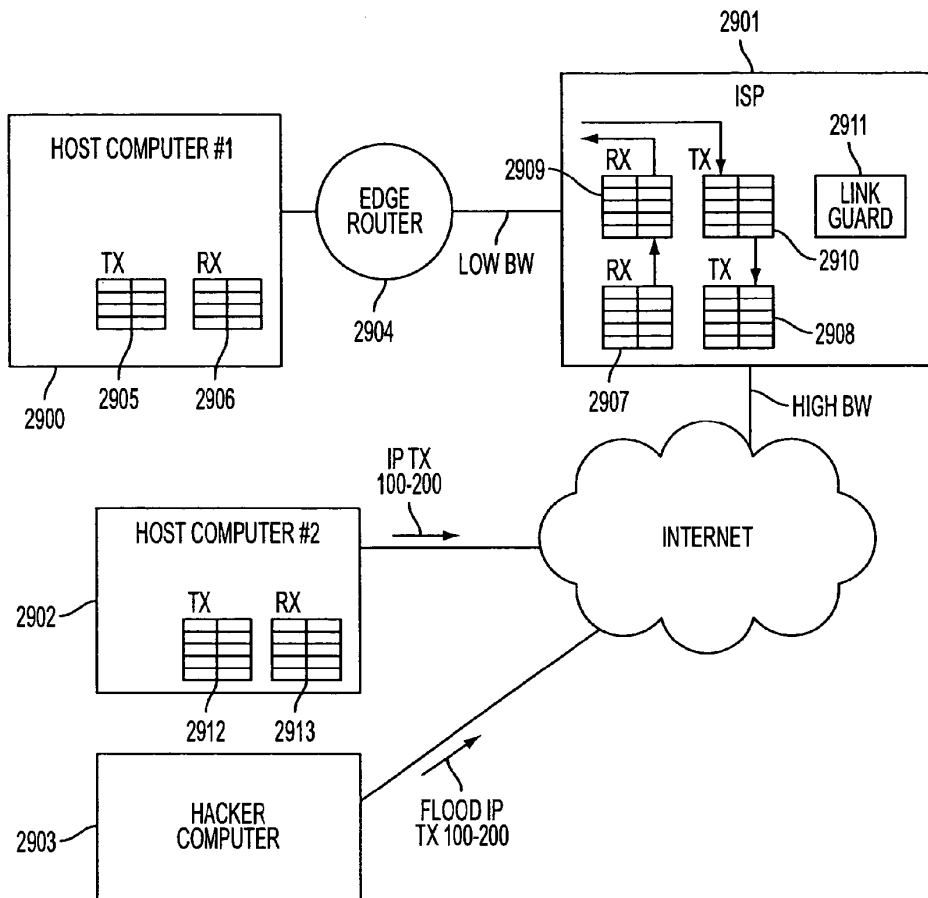


FIG. 29

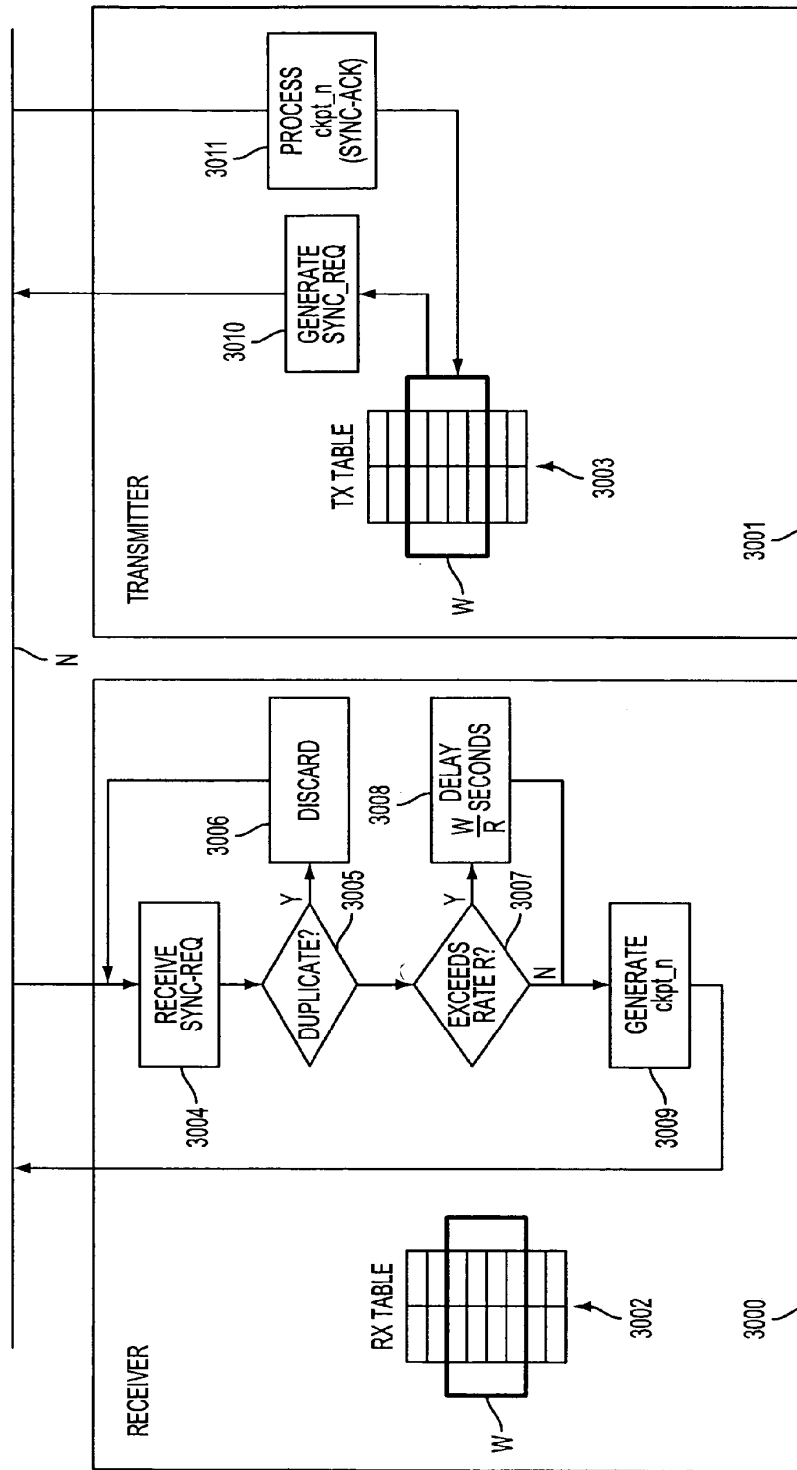


FIG. 30

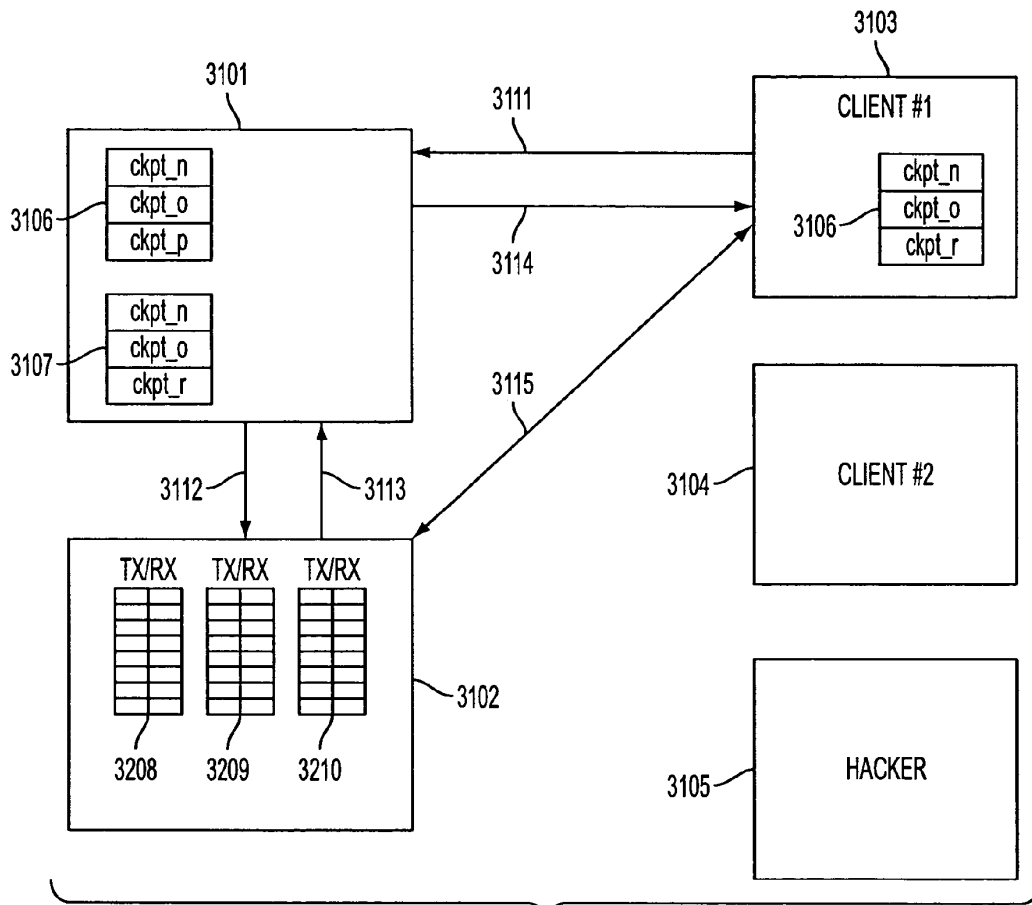


FIG. 31

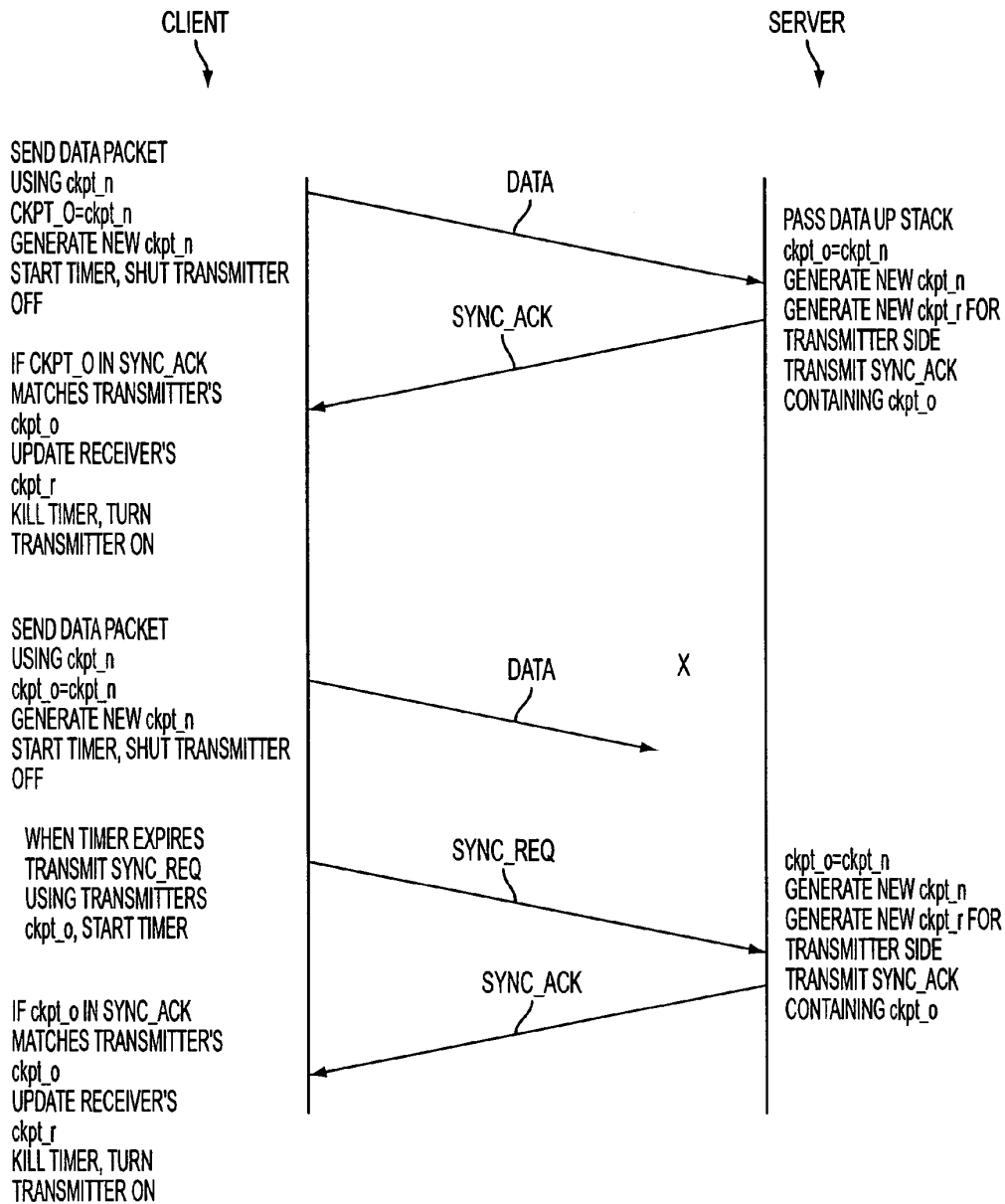


FIG. 32

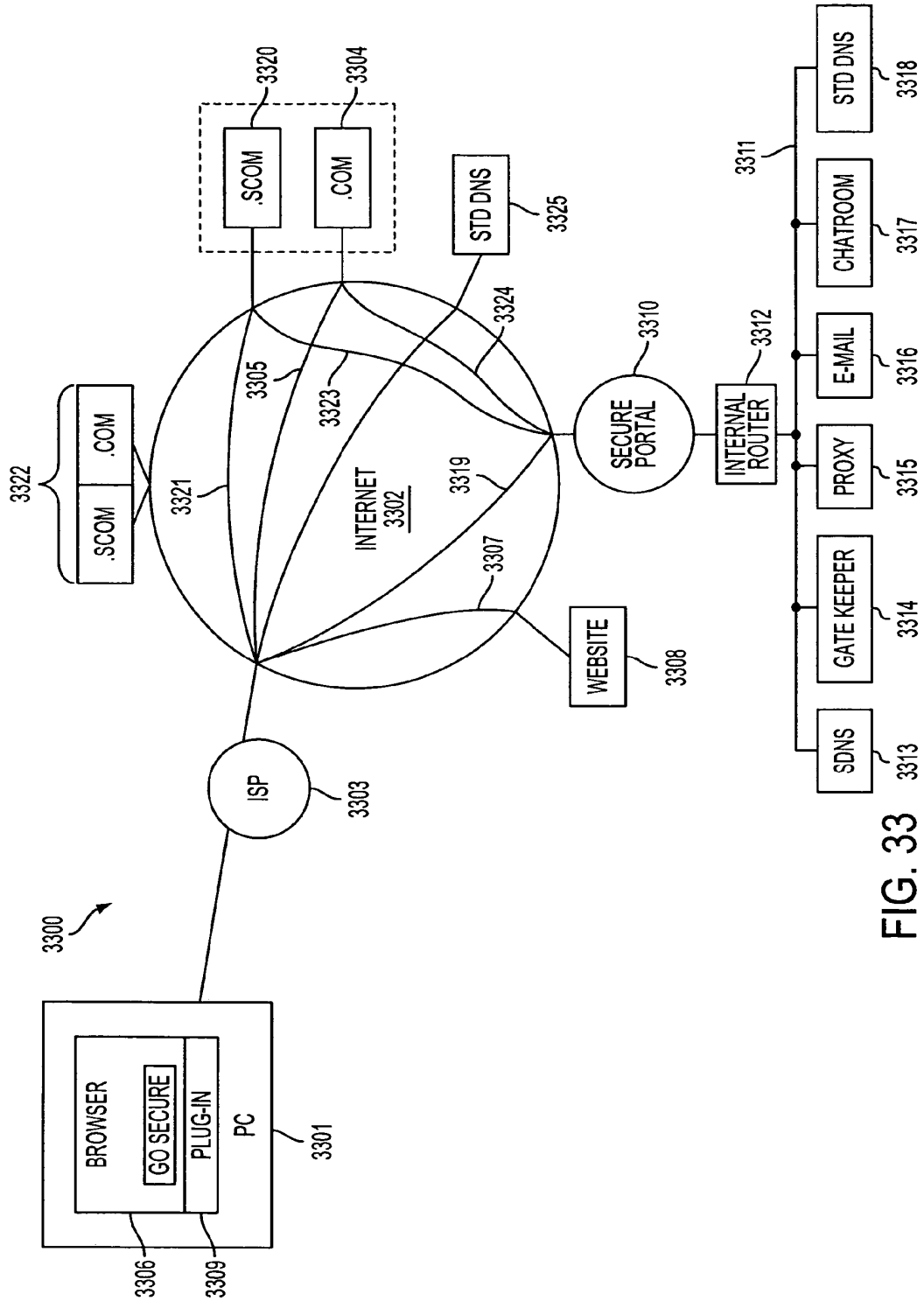


FIG. 33

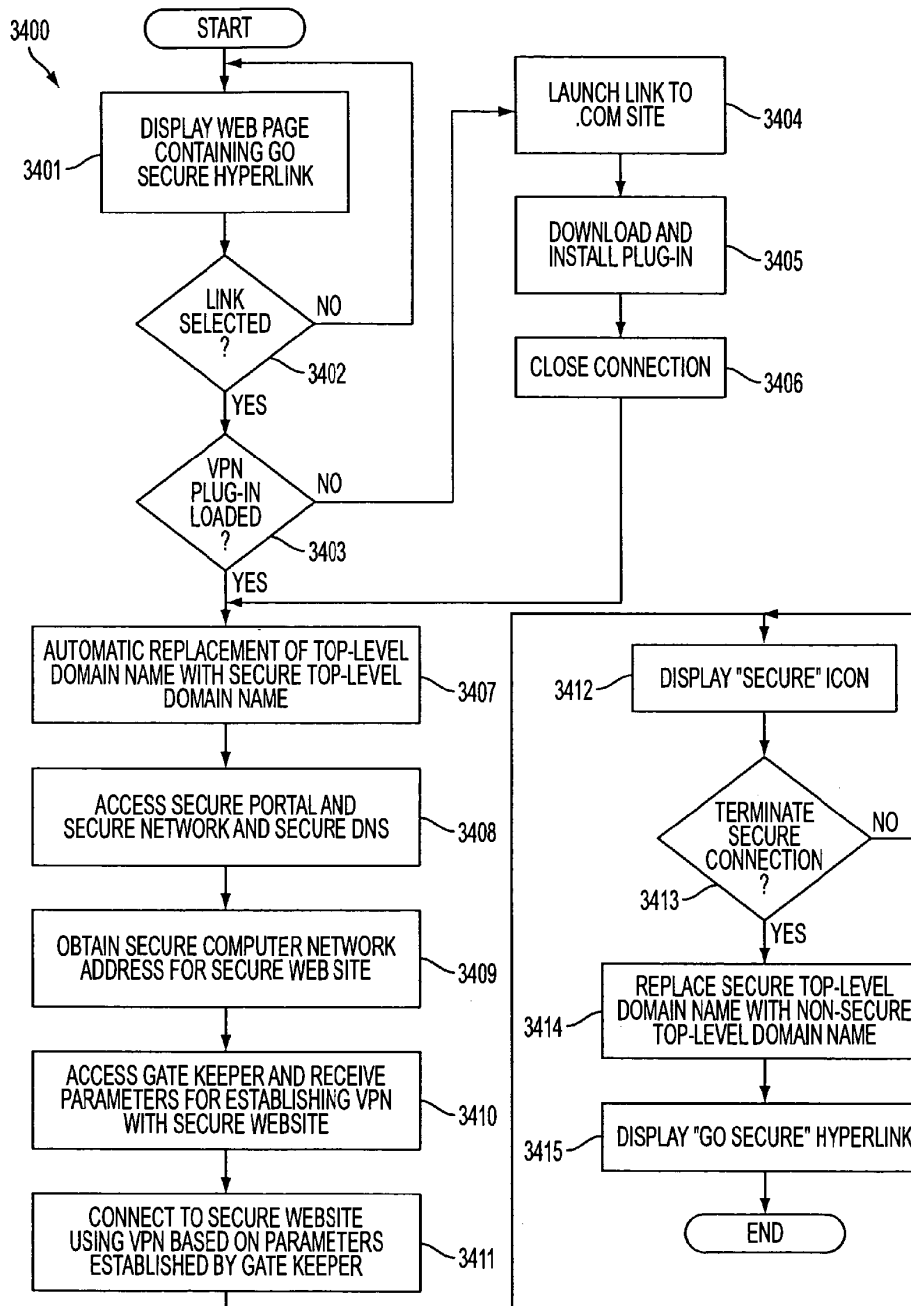


FIG. 34

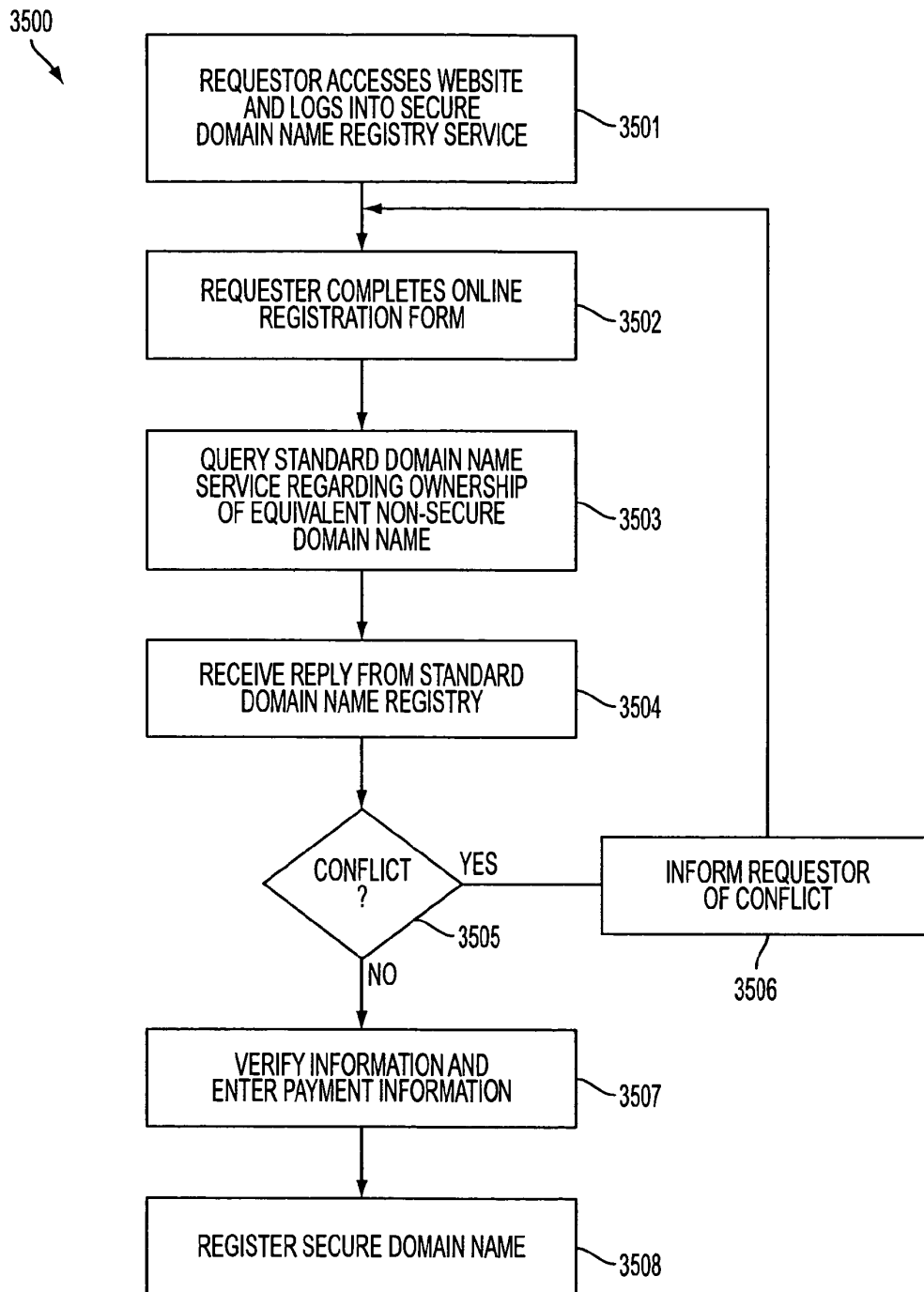


FIG. 35

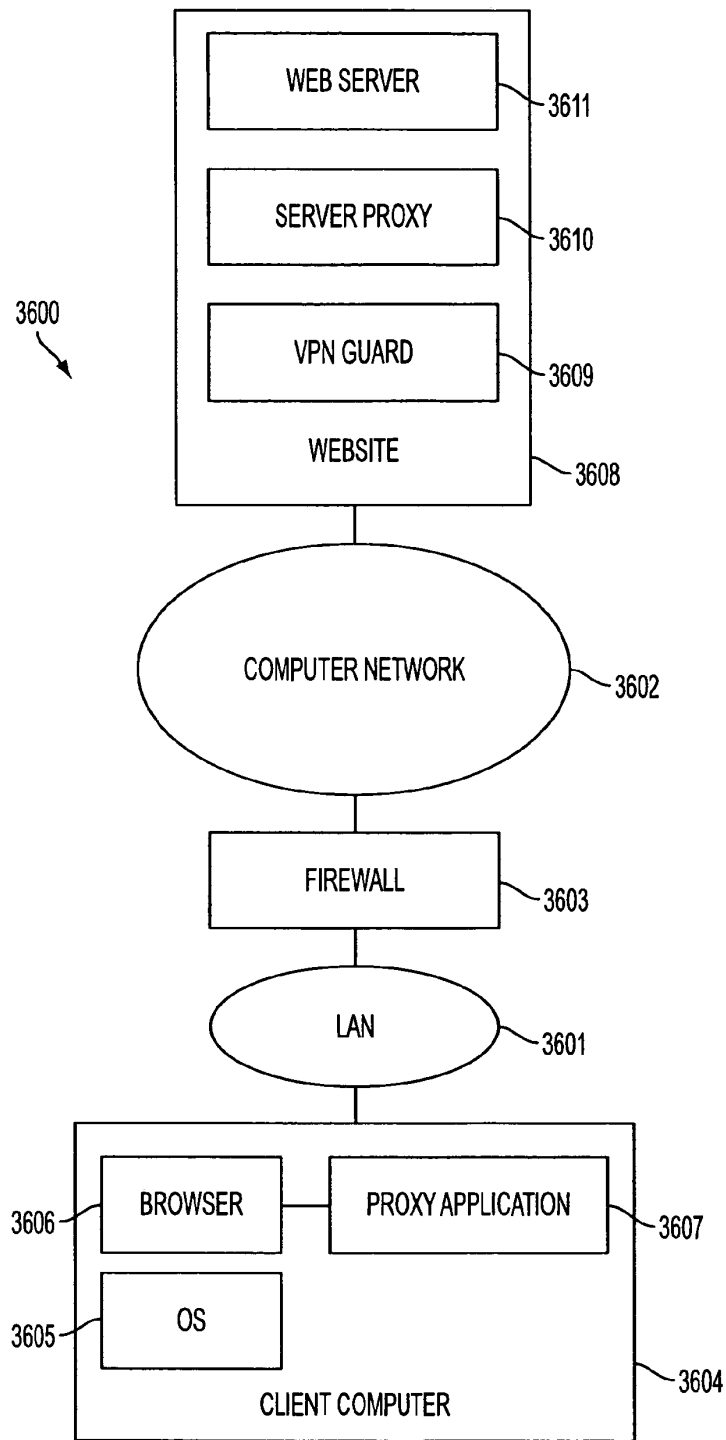


FIG. 36

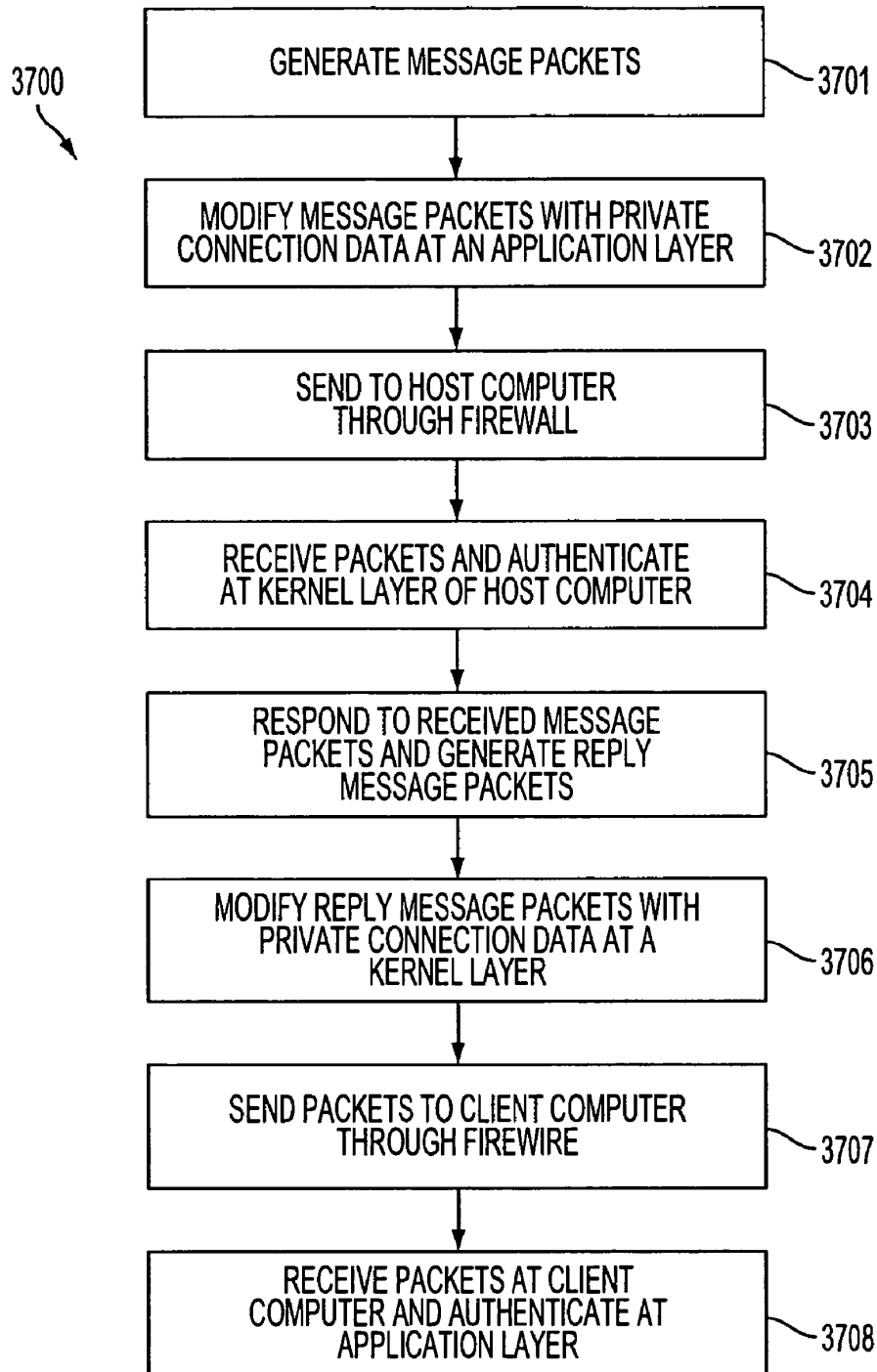


FIG. 37

**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, now abandoned which is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/504,783, filed on Feb. 15, 2000, now U.S. Pat. No. 6,502,135, issued Dec. 31, 2002, which 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 Nos. 60/106,261 (filed Oct. 30, 1998) and 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 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 24-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 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 Look-up 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 IPT 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

5

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

6

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 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. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

FIG. 12B 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. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

FIG. 22B 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

11

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. **3a**, to construct a series of TARP packets, a data stream **300** of IP packets **207a**, **207b**, **207c**, 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 **207a** 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 **207a–207c**, 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

12

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 **207a–207c** 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. **3b**, 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. **3b**. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of FIG. **3a**. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. **3a**. The remaining process is as shown in, and discussed with reference to, FIG. **3a**.

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 IPC 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) data-

grams 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 (fishbowed) 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.

15

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.

16

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 within 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 IP1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header gener-

ally includes a source hardware address **1101A** and a destination hardware address **1101B**; 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 W1 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 it 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.

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 $X_1, X_2, X_3 \dots X_k$ starting with seed X_0 using a recurrence

$$X_i = (a X_{i-1} + b) \text{ mod } c, \tag{1}$$

where a, b and c define a particular LCR. Another expression for X_i ,

$$X_i = ((a^i(X_0 + b) - b) / (a - 1)) \text{ mod } c \tag{2}$$

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:

$$X_i = (a^i(X_0(a-1) + b) - b) / (a-1) \text{ mod } c. \tag{3}$$

It can be shown that:

$$(a^i(X_0(a-1) + b) - b) / (a-1) \text{ mod } c = ((a^i \text{ mod } ((a-1)c) (X_0(a-1) + b) - b) / (a-1)) \text{ mod } c \tag{4}$$

$(X_0(a-1) + b)$ can be stored as $(X_0(a-1) + b) \text{ mod } c$, b as $b \text{ mod } c$ and compute $a^i \text{ mod } ((a-1)c)$ (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^m , the random number at the j^{th} checkpoint, as X_0 and n as i, a node can store $a^n \text{ mod } ((a-1)c)$ once per LCR and set

$$X_{j+1}^m = X_{n(j+1)}^m = ((a^n \text{ mod } ((a-1)c) (X_j^m(a-1) + b) - b) / (a-1)) \text{ mod } c, \tag{5}$$

to generate the random number for the $j+1^{\text{th}}$ 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:

$$X_i = (31 X_{i-1} + 4) \text{mod } 15. \tag{6}$$

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 $a^3=31^3=29791$, $c*(a-1)=15*30=450$ and $a^3 \text{mod}((a-1)c)=31^3 \text{mod}(15*30)=29791 \text{mod}(450)=91$. Equation (5) becomes:

$$(91(X_{i+3}+4)-4)/30 \text{mod } 15 \tag{7}$$

Table 1 shows the jump ahead calculations from (7). The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	$(X_i,30 + 4)$	$91 (X_i,30 + 4) - 4$	$((91 (X_i,30 + 4) - 4)/30$	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 $2 \times \text{WINDOW_SIZE} + \text{OoO}$ active addresses ($1 \leq \text{OoO} \leq \text{WINDOW_SIZE}$ and $\text{WINDOW_SIZE} \geq 1$). 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 $2 \times \text{WINDOW_SIZE}$ 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 $2 \times \text{WINDOW_SIZE} - \text{OoO}$ 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.

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. 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.

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. 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).

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. 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.

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:

$$P' = \alpha \times \text{MIN} + (1 - \alpha) \times P \tag{1}$$

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:

$$P' = \beta \times S + (1 - \beta) \times P \tag{2}$$

where β is a parameter such that $0 < \beta < 1$ 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 L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 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 L1; 0.375 for link L2, and 0.125 for link L3. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, $\alpha=0.75$ and $\beta=0.5$. 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 L1 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 L1 would be below THRESH (0.8). Consequently, link L1's traffic weight value would be reduced to 0.12825, while link L2's traffic weight value would be increased to 0.65812 and link L3's traffic weight value would be increased to 0.217938.

2. Link L2 and L3 remained healthy and link L1 stopped to synchronize. Then link L1's traffic weight value would be set to 0, link L2's traffic weight value would be set to 0.75, and link L3's traffic weight value would be set to 0.25.

3. Link L1 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.

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.

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.

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

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 "hopping blocks" 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

41

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

42

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 com-

puter 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 $M \times N \times W/R$ 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 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 $M \times N \times W/R$ 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 $(C-1)^{th}$ 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 T1 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 T1 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 server). 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 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 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 com-

51

puter 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

52

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 requester 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 requestor 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 3607 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 method for accessing a secure computer network address, comprising steps of:
 - receiving a secure domain name;
 - sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
 - receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 - sending an access request message to the secure computer network address using a virtual private network communication link.
2. The method according to claim 1, wherein the step of receiving the secure domain name includes steps of:
 - receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

57

automatically generating a secure domain name corresponding to the non-secure domain name.

3. The method according to claim 2, wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.

4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.

5. The method according to claim 4, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

6. The method according to claim 4, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

7. The method according to claim 4, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

8. The method according to claim 4, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

9. The method according to claim 4, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

10. The method according to claim 1, wherein the virtual private network includes the Internet.

11. The method according to claim 1, wherein the secure domain name has a top-level domain name that includes one of .com, .net, .org, .edu, .mil or .gov.

12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.

13. The method of claim 1,
 wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;
 wherein sending the query message comprises sending the query message at the client computer;
 wherein receiving the response message comprises receiving the response message at the client computer,
 wherein sending the access request message comprises sending the access request message at the client computer.

14. The method of claim 1, performed by a software module.

15. The method of claim 1, performed by a client computer.

16. The method of claim 2, wherein receiving the command comprises receiving the command at a client computer from a user.

17. A computer-readable storage medium, comprising:
 a storage area; and
 computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:
 receiving a secure domain name;
 sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;

58

receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
 sending an access request message to the secure computer network address using a virtual private network communication link.

18. The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:
 receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and
 automatically generating a secure domain name corresponding to the non-secure domain name.

19. The computer-readable medium according to claim 18, wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.

20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.

21. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

22. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

23. The computer-readable medium according to claim 20, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

24. The computer-readable medium according to claim 20, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

25. The computer-readable medium according to claim 20, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.

27. The computer-readable medium according to claim 17, wherein the secure domain name has a top-level domain name that includes one of .com, .net, .org, .edu, .mil or .gov.

28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.

29. The computer-readable medium according to claim 17,
 wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;
 wherein sending the query message comprises sending the query message at the client computer;

59

wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access request message comprises sending the access request message at the client computer.

30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.

31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.

32. The computer-readable medium according to claim 18, wherein receiving the command comprises receiving the command at a client computer from a user.

33. A data processing apparatus, comprising: a processor, and

memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

34. The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:

receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

60

automatically generating a secure domain name corresponding to the non-secure domain name.

35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.

36. The apparatus of claim 35, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

37. The apparatus of claim 35, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

38. The apparatus of claim 35, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

39. The apparatus of claim 35, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

40. The apparatus of claim 35, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

41. The apparatus of claim 33, wherein the secure domain name has a top-level domain name that includes one of .com, .snet, .sorg, .sedu, smil or .sgov.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,188,180 B2
APPLICATION NO. : 10/702486
DATED : March 6, 2007
INVENTOR(S) : Victor Larson et al.

Page 1 of 1

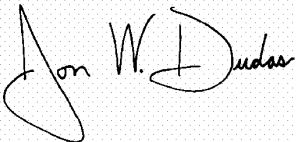
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

IN PATENT TITLE PAGE:

Item (75), Inventors, delete "Durham" and insert therefor -- Dunham --.

Signed and Sealed this

Seventh Day of August, 2007

A handwritten signature in black ink on a light gray dotted background. The signature reads "Jon W. Dudas" in a cursive style.

JON W. DUDAS

Director of the United States Patent and Trademark Office



US007188180C1

(12) **INTER PARTES REEXAMINATION CERTIFICATE** (0274th)
United States Patent
Larson et al. (10) **Number:** **US 7,188,180 C1**
(45) **Certificate Issued:** **Jun. 7, 2011**

- (54) **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**

4,933,846 A	6/1990	Humphrey et al.
4,988,990 A	1/1991	Warrior
5,276,735 A	1/1994	Boebert et al.
5,303,302 A	4/1994	Burrows

(Continued)

- (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)

FOREIGN PATENT DOCUMENTS

DE	199 24 575	12/1999
EP	0 814 589	12/1997
EP	836306 A1	4/1998
EP	0 838 930	4/1998
EP	0 858 189	8/1998

- (73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(Continued)

Reexamination Request:
No. 95/001,270, Dec. 8, 2009

OTHER PUBLICATIONS

Reexamination Certificate for:
Patent No.: **7,188,180**
Issued: **Mar. 6, 2007**
Appl. No.: **10/702,486**
Filed: **Nov. 7, 2003**

Exhibit 2 "Aventail Connect v.3.1/v2.6 Administrator's Guide", pp. 1-120, 1996-1999.

Exhibit 3, "Windows NT Server, Virtual Private Network: An Overview", pp. 1-28, 1998.

Exhibit 4, "Network Working Group Request For Comments 1035", pp. 1-56, 1987.

Certificate of Correction issued Aug. 7, 2007.

Related U.S. Application Data

(Continued)

- (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.

Primary Examiner—Andrew L Nalven

- (60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

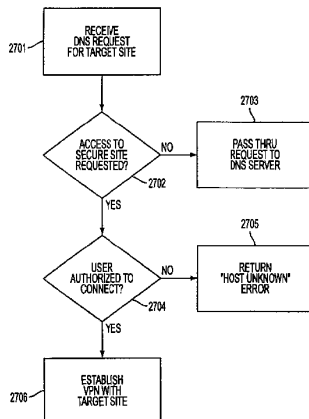
(57) **ABSTRACT**

- (51) **Int. Cl.**
G06F 15/173 (2006.01)

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.

- (52) **U.S. Cl.** **709/227; 709/228**
- (58) **Field of Classification Search** **709/227**
See application file for complete search history.

- (56) **References Cited**
U.S. PATENT DOCUMENTS
2,895,502 A 7/1959 Roper et al.



U.S. PATENT DOCUMENTS			
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
5,625,626	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
5,796,942	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.
5,918,019	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.
6,308,274	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.
6,430,155	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.
6,618,761	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.
6,752,166	B2	6/2004	Lull et al.
6,757,740	B1	6/2004	Parkh 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
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.
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			
GB		2 317 792	4/1998
GB		2 334 181 A	8/1999
JP		62-214744	9/1987
JP		04-363941	12/1992
JP		09-018492	1/1997
JP		10-070531	3/1998
WO		WO 9827783 A	6/1998

WO	WO 98/27783	6/1998
WO	WO 98 55930	12/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/17775	3/2000
WO	WO 0017775	3/2000
WO	WO 00/70458	11/2000
WO	WO 01/16766	3/2001
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

- Exhibit 5, "Kusur" Building and Managing Virtual Private Networks, pp. 1-396, 1998.
- Exhibit 6, "Kaufman et al.," Implementing IPsec, pp. 1-280, 1999.
- Exhibit 7, "James Galvin" Public Key Distribution Secure DNS, pp. 1-12, 1996.
- Exhibit 8A, Gauntlet Firewall for Windows NT Administrator's Guide, pp. 1-137, 1998-1999.
- Exhibit 8B, Gauntlet Firewall for windows NT Administrator's Guide, pp. 138-275, 1998-1999.
- Exhibit 9, "Windows NT Technical Support: Hands On, Self Paced Training for Supporting Version 4.0", pp. 1-106, 1998.
- Exhibit 10, Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, pp. 1-30, 1997.
- Exhibit 11, Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources, pp. 1-216, 2000.
- 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 Uezone, "Network Security", Japan, Nikkei McGraw-Hill, Dec. 5, 1958, First Edition, first copy, p. 102-108.
- 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 3-540-666.
- 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.freeswan.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.
- 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 (dated Nov. 13, 2002), International Application 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 conference on Communications architecture & 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.
- Fasbender, A. et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.
156. Finding Your Way Through the VPN Maze (1999) ("PGP").
- 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).
- 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.
- I. 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. 3, 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?0 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).
- Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX).
- Automotive 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 <http://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 1989 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 New Opportunities 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 Assurance Computer Systems (Jun. 2, 1997). (Syverson, Onion Routing).
- Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIG 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 <http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpfalse>). (NT Beta, Microsoft Prior Art VPN Technology).
- "What ports does SSL use" available at stason.org/TU-LARC/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). (DNS-SEC-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 3.1/2.6 Administrator'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-ietf-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, *Linus 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). (Bhattacharya 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 (JEFFX) 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 ANS IPsec Certificates. (Appendix, ANX).
- Assured Digital Products. (Assured Digital).
- 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).
- Publicly 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-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).
- Darrel 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.mspix> (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.).
- Microsoft Corp. windows NT Server Product Documentation: Administration Kit Guide—Connection Manager, available at <http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspix> (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](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](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](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](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](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](http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx) (Suhy).
126. Aaron Skonnard, *Essential WinNet* 313–423 (Addison Wesley Longman 1998) (Essential WinNet).
- Microsoft Corp., Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) available at [http://msdn2.microsoft.com/en-us/library/ms811078\(printer\).aspx](http://msdn2.microsoft.com/en-us/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.mspix> (Internet Connection Services I).
- Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, available at <http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspix> (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/depoy/deploy5/appendb.mspix> (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.mspix> (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](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.mspix> (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.mspix> (NT4VPN) (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/rrascho01.mspix> (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.mspix> (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 SSH 2.0 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. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical 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 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).
- WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Release 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, *IIS 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. Linsenhardt, *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., filed 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/bookid_762/viewer_r.asp?book/id=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.
- 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. 1989); 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").
- 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.

1
INTER PARTES
REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 316

NO AMENDMENTS HAVE BEEN MADE TO
THE PATENT

2
AS A RESULT OF REEXAMINATION, IT HAS BEEN
DETERMINED THAT:
The patentability of claims 1, 4, 10, 12-15, 17, 20, 26,
28-31, 33 and 35 is confirmed.
5 Claims 2, 3, 5-9, 11, 16, 18, 19, 21-25, 27, 32, 34 and
36-41 were not reexamined.

* * * * *

Exhibit E1

Claim charts applying Lendenmann as a primary reference to the '180 patent.

EXHIBIT E-1
Lendenmann

Contents

Chart E-1.1:	Detailed support for Proposed Rejection #1, showing that claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102(b).....	2
Chart E-1.2:	Detailed support for Proposed Rejection #2, showing that claims 5, 21, and 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103.....	68
Chart E-1.3:	Detailed support for Proposed Rejection #3, showing that claims 7, 23, and 38 are obvious over Lendenmann in view of Martin under 35 U.S.C. § 103.	73
Chart E-1.4:	Detailed support for Proposed Rejection #4, showing that claims 11, 27 and 41 are obvious over Lendenmann under 35 U.S.C. § 103.	77

EXHIBIT E-1
Lendenmann

Section 1 – Anticipation

Chart E-1.1: Detailed support for Proposed Rejection #1, showing that claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102(b).

“Lendenmann”: Rolf Lendenmann, *Understanding OSF DCE 1.1 for AIX and OS/2*, IBM International Technical Support Organization (Oct. 1995).

Lendenmann is a printed publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of Oct. 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of Lendenmann is attached as Exhibit D-1.

As potentially helpful guidance in giving the claims the broadest reasonable interpretation consistent with the specification, the following analysis makes occasional reference to the Patent Owner's prior characterizations of the claims in the first reexamination, and to the claim interpretation from prior litigation involving the '180 patent:

- Reexamination of US 7,188,180, Control No. 95/001,270, Patent Owner Response filed May 24, 2010 [*hereinafter* “Patent Owner Response”]. A copy of the Patent Owner Response is included in Exhibit B-3.
- *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009) [*hereinafter* “E.D. Tex. Order”]. A copy of the E.D. Tex. Order is attached as Exhibit B-4.

The following analysis also refers to the following documents to assist (i) interpreting the claim language under the broadest reasonable interpretation and (ii) understanding the teachings of Lendenmann in accordance with MPEP 2131.01:¹

- “RFC 793”: Information Sciences Institute, “Transmission Control Protocol,” DARPA Internet Program Protocol Specification RFC 793 (Sept. 1981).

RFC 793 is a printed publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of RFC 793 is attached as Exhibit D-6.

¹ A second or subsequent reference may be referenced in a rejection under 35 U.S.C. § 102 “when the extra references are cited to: (A) Prove the primary reference contains an ‘enabled disclosure;’ (B) Explain the meaning of a term used in the primary reference; or (C) Show that a characteristic not disclosed in the reference is inherent.” MPEP 2131.01.

EXHIBIT E-1
Lendenmann

- “RFC 1034”: P. Mockapetris, “Domain Names – Concepts and Facilities,” RFC 1034 (Oct. 1987).

RFC 1034 is a publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of RFC 1034 is attached as Exhibit D-10.

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>[1.0] A method for accessing a secure computer network address, comprising steps of:</p>	<p>[1.0] <i>A method for accessing a secure computer network address, comprising steps of:</i></p> <p>Lendenmann teaches accessing a secure computer network address.</p> <p>Lendenmann describes the Distributed Computing Environment (DCE) software system, which includes the capability of performing a remote procedure call (RPC) to perform communication between a client and a server:</p> <p>1.4.1.1 The Client/Server Model In the client/server model, a distributed application is divided into two parts, <i>client</i> and <i>server</i>. In simple terms, the client is the entity that initiates the request for a service. The server is the entity that handles the request for a service. ...</p> <p>1.4.1.2 The Remote Procedure Call Model In this model, the client makes what looks like a local procedure call. This procedure call is translated, and network communications are handled by the RPC mechanism. The <i>server receives a request and executes the procedure, returning the results to the client.</i> DCE RPC is an</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>implementation of this model and is used by most of the other DCE technology components for their network communications.</p> <p>(Lendenmann at 8-9, bold-italic emphasis added.)</p> <p>Lendenmann further describes using a remote procedure call in conjunction with security services. For example, Lendenmann describes how an authenticated remote procedure call allows a client to access a resource that requires authorization:</p> <p style="padding-left: 40px;">DCE RPC supports authenticated communications between clients and servers. Authenticated RPC is provided by the RPC runtime facility and <i>works with the authentication and authorization services</i> provided by the DCE security service.</p> <p>(Lendenmann at 191, emphasis added.)</p> <p>Lendenmann describes how the various services provided by DCE support secure communications and operations:</p> <p style="padding-left: 40px;">The DCE Security component comprises three services running on the security server and several other facilities. Most of the DCE security is related to the concept of a principal. A <i>principal</i> is an entity that can be securely identified and can engage in a trusted communication. A principal usually represents a user, a network service, a particular host, or cell. Each principal is uniquely named and identified by its principal UUID. A record for each principal containing the name, the private keys and the expiration date is kept in the registry database on a highly secure system. The three services are:</p> <ul style="list-style-type: none">· <i>Registry Service (RS)</i> — A replicated service which maintains the cell's security database. This database contains entries for accounts, principals, groups, organizations, and administrative policies.· <i>Authentication Service (AS)</i> — Used to verify the identity of

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>principals. It contains a Ticket-Granting Service (TGS) which grants tickets to these principals and services <i>so that they can engage in a secure communication.</i></p> <p>· <i>Privilege Service (PS)</i> — Certifies a principal’s credentials that are going to be forwarded in a secure way to DCE servers. The credentials (see EPACs below) allow the target server to check the principal’s access rights to resources.</p> <p>(Lendenmann at 45, italics in original, bold-italic emphasis added.)</p> <p>As an example of the kinds of security available using DCE, Lendenmann describes encrypting communications between a client and server:</p> <p>The following protection levels are available:</p> <p>...</p> <ul style="list-style-type: none"> · CDMF Privacy. <i>Encrypts</i> RPC arguments and data in each call using CDMF. · Packet Privacy. <i>Encrypts</i> RPC arguments and data in each call using DES. <p><i>Encryption is done with the session key, which is only known by the client and the server</i> for which the service ticket was issued.</p> <p>(Lendenmann at 192, emphasis added.)</p> <p>It is understood that engaging in secure communication, such as by encrypting traffic between a client and server, includes “accessing a secure computer network address.”</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10.)</p> <p>Thus, Lendenmann teaches a “method for accessing a secure computer network address” as recited in the claim.</p>
<p>[1.1] receiving a secure domain name;</p>	<p>[1.1] <i>receiving a secure domain name</i></p> <p>Lendenmann discloses “receiving a secure domain name.”</p> <p>Specifically, Lendenmann teaches that a directory service allows a user to identify and locate a server by name, even when the server’s network address might change:</p> <p style="padding-left: 40px;">The directory service is the process that makes it possible for the user to <i>locate objects in the network</i> without knowing their physical location. It hides from the user the distributed nature of the environment. It is like a telephone directory assistance service that provides the phone number when given a person’s name.</p> <p>(Lendenmann at 19.)</p> <p style="padding-left: 40px;">DCE Naming Service provides a naming model throughout the distributed environment. This model allows users to <i>identify, by name, resources, such as servers</i>, files, disks, or print queues, and gain access to them without needing to know where they are located in a network. Further, users can continue referring to a resource by the same name <i>even when a characteristic of the resource changes, such as its network address</i>.</p> <p>(Lendenmann at 22.)</p> <p>Lendenmann further teaches that name resolution services are provided by a Cell Directory Service (CDS):</p> <p style="padding-left: 40px;">The directory service component that controls names inside a cell is called the <i>Cell Directory Service (CDS)</i>. The CDS</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>stores names of resources in that cell so that when given a name, CDS <i>returns the network address of the named resource</i>.</p> <p>(Lendenmann at 21.)</p> <p>Lendenmann teaches that each computer in a network includes a Cell Directory Service clerk (CDS clerk) that receives network name look-up requests and passes the request on to a CDS server:</p> <p>Each DCE machine runs a CDS clerk which intermediates between the client applications and the CDS server. <i>The clerk receives a request</i> from the DCE application to store or retrieve information and sends the request to the CDS server for processing.</p> <p>(Lendenmann at 29, emphasis added.)</p> <p>Lendenmann illustrates in Fig. 15 how the clerk acts on behalf of the application to look-up information requested:</p> <p>Figure 15 shows the look-up process:</p> <ol style="list-style-type: none">1. The client application on node 1 <i>sends a look-up request to the local clerk</i>.2. The clerk checks its cache and, not finding the name there, contacts the server on node 2.3. The server checks to see if the name is in its clearinghouse.4. The name exists in the clearinghouse; so the server gets the requested information.5. The server returns the information to the clerk on node 1.6. The clerk caches the information and passes the requested data to the client application.

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180* Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102

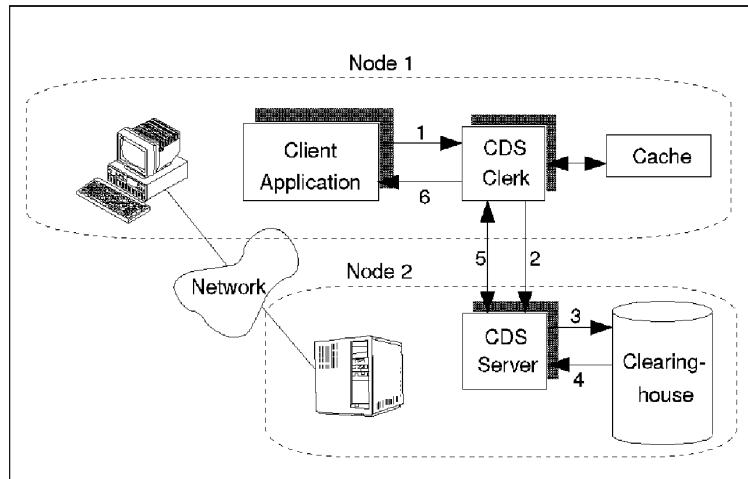


Figure 15. CDS Components Performing a CDS Look-up

(Lendenmann at 29-30, emphasis added.)

Lendenmann further discloses that the names of client and server computers are secure domain names. For example, Lendenmann describes supporting both the X.500 and Internet Domain Name Service (DNS) naming schemes:

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.)

As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the patent owner asserts that the phrase “secure domain name” refers to a name that “cannot be resolved by a conventional domain name service.” (Patent Owner Response at 6.)

Lendenmann provides examples of X.500 names that could not be resolved by a conventional domain name server:

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>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 <code>././susbsys/PrintQ</code>. The prefix (<code>././</code>) 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 (<code>=</code>). The abbreviation of each block stands for country (C), organization (O), organizational unit (OU), and common name (CN, not shown).</p> <p>(Lendenmann at 23.)</p> <div style="text-align: center;"> <p>Cell name CDS name</p> <p>-----</p> <p><code>././C=US/O=IBM/OU=ITSO/susbsys/PrintQ</code></p> <p>Lendenmann Fig. 9</p> </div> <p>Neither the local name example (“<code>././susbsys/PrintQ</code>”) nor the global name example (“<code>././C=US/O=IBM/OU=ITSO/susbsys/PrintQ</code>”) are conventional domain names.</p> <p>Those of skill in the art would have understood that a conventional domain name would conform to the rules outlined in RFC 1034, “Domain Concepts and Facilities.” RFC 1034 defines the domain name service used to identify hosts on the Internet, which is the type of conventional domain name service described in the ’180 patent specification. See, for example, the ’180 patent at 39:45-52, describing a conventional domain name service used to resolve the IP address of “Yahoo.com.”</p> <p>RFC 1034 requires that a domain name “must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphen.” (RFC 1034 at 11.) Notably, the example X.500 names in Lendenmann <i>do not</i> start with a letter, and they include such disallowed characters as the forward slash (<code>/</code>) and equals sign (<code>=</code>). Lendenmann’s X.500 names are not conventional domain names and could not be resolved by a conventional domain name service.</p> <p>Thus, under at least the Patent Owner’s interpretation of the claim scope,</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>these example names are each a “secure domain name.”</p> <p>Lendenmann further describes setting security requirements and requiring authentication before allowing a user to resolve secure network names into their corresponding secure network addresses:</p> <p>The CDS, as any other DCE service, is integrated into the security service. The CDS server <i>only completes an operation over the clearinghouse if the user is authenticated and authorized</i> 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.</p> <p>CDS authorization allows you to <i>control user access to</i>:</p> <ul style="list-style-type: none"> · <i>Names in the namespace</i>, including clearinghouses, directories, object entries, soft links, and child pointers · Execution of privileged CDS clerk and server commands <p>(Lendenmann at 34, emphasis added.)</p> <p>Because a user must be authenticated and authorized in order to resolve a name, the name is a “secure domain name.” For example, a client cannot resolve the network address of the name unless it is authorized, and therefore unauthorized clients cannot communicate with the corresponding network address (since authorized clients cannot learn what that address is.)</p> <p>As evidence that this interpretation is also within the broadest reasonable interpretation of a person of skill in the art, note that the patent owner asserted that the phrase “secure domain name” may alternatively refer to a name of a computer with which no communications are possible without authorization. (Patent Owner Response at 6-7.)</p> <p>In addition, a federal court interpreted the phrase “secure domain name” to refer to a “domain name that corresponds to a secure computer network address.” (E.D. Tex. Opinion at 31.) The court interpreted a</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>secure computer network address to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (<i>Id.</i> at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10)</p> <p>Thus, Lendenmann teaches “receiving a secure domain name” as recited in the claim.</p>
<p>[1.2a] sending a query message to a secure domain name service, [1.2b] the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[1.2a] <i>sending a query message to a secure domain name service</i></p> <p>As analyzed above in portion [1.1], Lendenmann teaches using secure domain names, such as names under the X.500 naming standard. Lendenmann teaches that a client resolves such secure domain names into corresponding secure network addresses by sending a query to a suitable domain name service, such as the Cell Directory Service (CDS):</p> <p style="padding-left: 40px;">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 <i>when given a name, CDS returns the network address</i> of the named resource.</p> <p>(Lendenmann at 21, emphasis added.)</p> <p>Lendenmann further illustrates in Fig. 15 how a CDS clerk on the client sends the query message to a CDS Server:</p> <p style="padding-left: 40px;">Each DCE machine runs a CDS clerk which intermediates between the client applications and the CDS server. The clerk receives a request from the DCE application to store or retrieve information and <i>sends the request to the CDS server</i> for processing....</p> <p>Figure 15 shows the look-up process:</p> <p>...</p> <p>2. The clerk checks its cache and, not finding the name there, <i>contacts the server</i> on node 2.</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180* Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102

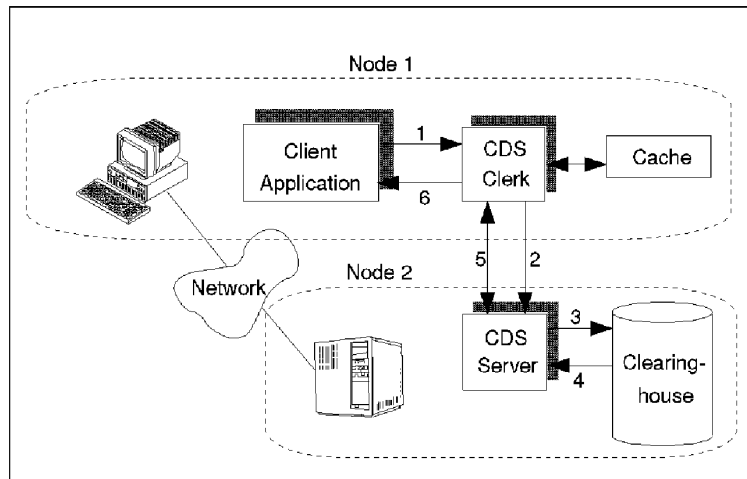


Figure 15. CDS Components Performing a CDS Look-up

(Lendenmann at 29-30, emphasis added.)

Lendenmann also describes how the CDS Server may refer queries for a foreign name to Global Directory Agent (GDA) or a Global Directory Service (GDS), but that such other servers are not required for names defined within the CDS. The GDA recognizes the type of name used, and is therefore aware of whether or not the request is directed to a secure domain name:

If it is a foreign name, the CDS server returns the address of a Global Directory Agent (GDA) contained in the CDS_GDAPointers attribute of its root directory. The CDS clerk sends the request to the GDA. ...

The *GDA recognizes the type of name* that is used. *If it receives an X.500 cell name, it passes the request to the Global Directory Service (GDS) client* in its own cell. The GDS client passes the request to a GDS server, which can be anywhere in the whole global network.

(Lendenmann at 26.)

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>The advantage, for the time being, is that intercell communication can now be defined within CDS. <i>Global naming services (GDS or DNS) need not be involved.</i></p> <p>(Lendenmann at 25, emphasis added.)</p> <p>The Cell Directory Service (CDS) that resolves X.500 domain names, either directly and by consulting the Global Directory Service (GDS), is a “secure domain name service,” as recited in the claim.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserts that a “secure domain name service” is a name service that “is different from a conventional domain name service.” (Patent Owner Response at 8.) As analyzed above in portion [1.1], the Cell Directory Service (CDS) can resolve domain names that are not conventional domain names, and therefore the Cell Directory Service (CDS) is different from a conventional domain name service.</p> <p>Thus, Lendenmann teaches “sending a query message to a secure domain name service” as recited in the claim.</p> <hr/> <p>[1.2b] <i>the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name</i></p> <p>Lendenmann teaches requesting a secure computer network address corresponding to the secure domain name:</p> <p><i>A client can find a server by asking the CDS for the location of a server</i> that handles the interface that the client is interested in.</p> <p>(Lendenmann at 182, emphasis added.)</p> <p>And as analyzed above in portion [1.1] and [1.2a], Lendenmann teaches that the Cell Directory Service (CDS) provides a network address in response to a name query:</p>

EXHIBIT E-1
Lendenmann

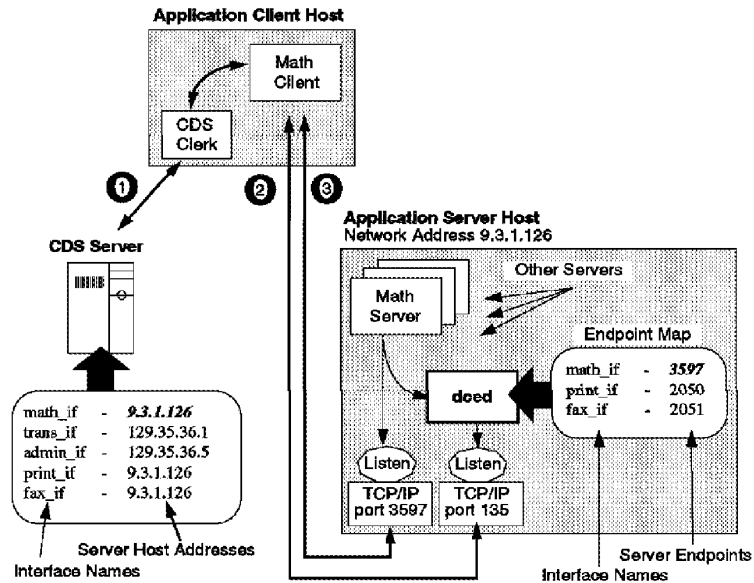
U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>The directory service component that controls names inside a cell is called the Cell Directory Service (CDS). The CDS stores names of resources in that cell so that <i>when given a name, CDS returns the network address</i> of the named resource.</p> <p>(Lendenmann at 21, emphasis added.)</p> <p>And as analyzed above in portion [1.1], a name as taught by Lendenmann, such as an X.500 domain name, is a “secure domain name.”</p> <p>Lendenmann further teaches that the network address returned by the Cell Directory Service (CDS) is a “secure computer network address.” Lendenmann describes the importance of security in a network environment, and teaches using the DCE Security Service to make applications and products secure:</p> <p style="padding-left: 40px;">Security is one of the main reasons why customers are interested in DCE. Developers can use the DCE Security Service to make their distributed client/server applications or products secure.</p> <p>(Lendenmann at 41.)</p> <p>For example, Lendenmann teaches that a client may require authorization before being allowed to receive a network address from the Cell Directory Service (CDS):</p> <p style="padding-left: 40px;">The CDS, as any other DCE service, is integrated into the security service. <i>The CDS server only completes an operation over the clearinghouse if the user is authenticated and authorized</i> 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.</p> <p>CDS authorization allows you to <i>control user access to:</i></p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<ul style="list-style-type: none"> · <i>Names in the namespace</i>, including clearinghouses, directories, object entries, soft links, and child pointers · Execution of privileged CDS clerk and server commands <p>(Lendenmann at 34, emphasis added.)</p> <p>Since only authorized users and clients are permitted to obtain a network address from the CDS server, it is understood that unauthorized users and clients cannot communicate with or access the network address. Thus, Lendenmann teaches that only authorized clients and users can communicate with or access the network address associated with a secure domain name.</p> <p>In addition to requiring authorization to obtain a network address, Lendenmann further teaches that a client may require authorization in order to access resources provided by the server at the network address. For example, Lendenmann describes how a client may use a remote procedure call (RPC) to request a service from a server whose address was obtained from the Cell Directory Service (CDS):</p> <p style="padding-left: 40px;">Figure 68 illustrates a simplified process of a client searching for a server. It performs the following steps:</p> <ol style="list-style-type: none"> 1. Looking up a binding in CDS The client <i>sends a request</i> to its local CDS client (cdsclerk) <i>to look up an entry in the name space....</i> 2. Contacting the remote endpoint mapper ... 3. <i>Executing the RPC</i> With the fully bound handle, the client's RPC runtime then directly calls the server process listening to the endpoint.... <p>(Lendenmann at 190-91, emphasis added.)</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180* Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102



Lendenmann Fig. 68 (at 190)

Lendenmann further describes the security features implemented by a server to ensure that a client accessing a remote procedure call (RPC) is authorized:

The server can ask the RPC runtime for the privileges associated with a client. *Authenticated RPC supports the following operations for making client authorization information available to servers* for access checking:

- None. No authorization information is provided to the server.
- Name. Only the client principal name is provided to the server. This type of authorization is called name-based authorization.
- DCE. *The client's DCE Extended Privilege Attribute Certificate (EPAC) is provided to the server* with each remote procedure call made using the binding parameter. The EPAC contains the principal name and a list of

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>groups of which the principal is member. The EPAC also contains the name and group memberships of a principal in the delegation chain and any extended attributes that apply to the principal.</p> <p>(Lendenmann at 193.)</p> <p>Lendenmann also teaches that the client’s authorization information in the Extended Privilege Attribute Certificate (EPAC) is encrypted, along with the remote procedure call itself:</p> <p>The client RPC runtime requests a service ticket from the Security Service. This <i>ticket contains the client’s extended privilege attribute certificate (EPAC)</i> and a session key for the upcoming client/server communication. The EPAC contains the principal name and groups of which this principal is a member. <i>This ticket is encrypted</i> with the server’s session key. So, the client cannot decrypt and change it to its own liking. Together with the (unreadable) ticket, the client also is sent the session key. Of course, this communication between client and Security Service is itself encrypted.</p> <p>The client RPC runtime <i>encrypts the RPC call</i> with the session key and sends it to the server’s runtime together with the ticket. The server immediately challenges the client by sending it a randomly generated number which the client has to encrypt with the session key and return to the server.</p> <p>The server’s runtime obtains the server’s key from the local keytab file and decrypts the ticket, thereby learning the session key and the client’s EPAC. The random number is decrypted, and if it matches, everything is set for authenticated RPC. The session key is used in further communication over this binding.</p> <p>(Lendenmann at 194.)</p> <p>Thus, Lendenmann teaches that communication with the server providing</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>the remote procedure call requires authentication, authorization, and encryption. Accordingly, the network address of a server providing a remote procedure call as described in Lendenmann is a “secure computer network address,” under at least the broadest reasonable interpretation.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserted that a secure computer network address is an address that requires authorization for access or that requires authorization communication for a client computer to communicate with it. (See, for example, Patent Owner Response at 6 stating that “the computers ... themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them.”)</p> <p>In addition, a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (Id. at 10.)</p> <p>Thus, Lendenmann teaches “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.3] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain</p>	<p>[1.3] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name</i></p> <p>Lendenmann discloses that the Cell Directory Service (CDS) (the “secure domain name service,” as analyzed in portion [1.2a]) returns a response that includes the secure computer network address for the secure domain name:</p> <p>The directory service component that controls names inside a</p>

EXHIBIT E-1
Lendenmann

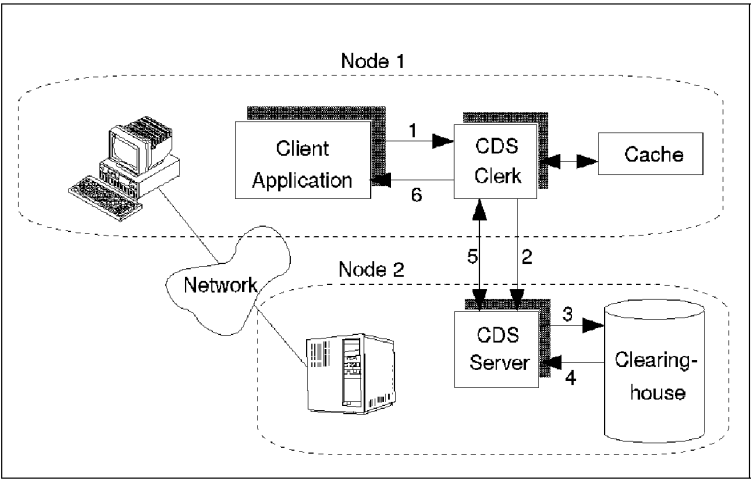
<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>name;</p>	<p>cell is called the Cell Directory Service (CDS). The CDS stores names of resources in that cell so that when given a name, <i>CDS returns the network address of the named resource.</i></p> <p>(Lendenmann at 21, emphasis added.)</p> <p>Continuing the specific example of Fig. 15 previously discussed in portions [1.1] and [1.2], Lendenmann teaches returning the information associated with the name provided earlier in the process:</p> <p>Figure 15 shows the look-up process:</p> <p>...</p> <ol style="list-style-type: none"> 3. The server checks to see if the name is in its clearinghouse. 4. The name exists in the clearinghouse; so the server gets the requested information. 5. <i>The server returns the information to the clerk</i> on node 1. <p>...</p>  <p><i>Figure 15. CDS Components Performing a CDS Look-up</i></p> <p>(Lendenmann at 29-30, emphasis added.)</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>Lendenmann specifically discloses that the information associated with a name in the CDS includes the associated server’s network address:</p> <p style="padding-left: 40px;">CDS stores the names and attributes of resources in the local cell. Although users are free to define their own objects and attributes, <i>in most cases the attributes store network address of servers</i> that provide access to the resources. The address attribute is called CDS_Towers and can contain several addresses of compatible servers.</p> <p>(Lendenmann at 33, emphasis added.)</p> <p>As previously analyzed in portion [1.3], a network address as described in Lendenmann is a “secure computer network address,” under at least the broadest reasonable interpretation. And as previously analyzed in portion [1.1, a name as described in Lendenmann is a “secure domain name,” under at least the broadest reasonable interpretation.</p> <p>Thus, Lendenmann teaches “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.4a] and sending an access request message to the secure computer network address [1.4b] using a virtual private network communication link.</p>	<p>[1.4a] and sending an access request message to the secure computer network address</p> <p>Lendenmann teaches sending an access request message to the secure computer network address. Specifically, Lendenmann teaches that a client can send a remote procedure call (RPC) to a server:</p> <p style="padding-left: 40px;">Distributed client/server applications in DCE use remote procedure calls (RPCs) to make function calls (transparently) across a network. Other DCE services also use RPCs; they are also client/server applications. RPC is the basis for DCE.</p> <p style="padding-left: 40px;">...</p> <p style="padding-left: 40px;">The RPC application has two sides: the client side which calls the remote procedure and the server side which executes the procedure in its own address space. Clients and servers can be on different computers linked by communications</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>networks.</p> <p>(Lendenmann at 173.)</p> <p>Lendenmann teaches that the client locates the server for a particular remote procedure call using the Cell Directory Service (CDS), which was analyzed above in portions [1.1]–[1.3]:</p> <p>The process of finding the server and <i>establishing a relationship over a communication link between the client and server RPC</i> 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. <i>A client can find a server by asking the CDS for the location of a server</i> that handles the interface that the client is interested in.</p> <p>(Lendenmann at 182, emphasis added.)</p> <p>As previously analyzed in portion [1.2], the server is located at a secure computer network address.</p> <p>Lendenmann further teaches that the remote procedure call (RPC) is sent to the server in encrypted form:</p> <p>The client RPC runtime <i>encrypts the RPC call</i> with the session key <i>and sends it to the server's runtime</i> together with the ticket. The server immediately challenges the client by sending it a randomly generated number which the client has to encrypt with the session key and return to the server.</p> <p>(Lendenmann at 194, emphasis added.)</p> <p>The encrypted RPC call sent to the server is “an access request message to the secure computer network address” as recited in the claim.</p> <p>Lendenmann further explains that an the RPC call includes the client’s</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>authorization information that allows the server to evaluate whether the client is permitted to access the requested resource at the server:</p> <p>Authorization is the mechanism that <i>allows the server to control client access</i> to a resource. The authorization process is application dependent. It is up to the server side of the application to implement the appropriate authorization checking it needs. The authorization process involves the matching of clients’ privilege attributes against the permissions associated with an object.</p> <p>The server can ask the RPC runtime for the privileges associated with a client. <i>Authenticated RPC supports the following operations for making client authorization information available to servers for access checking:</i></p> <ul style="list-style-type: none"> · None. No authorization information is provided to the server. · Name. Only the client principal name is provided to the server. This type of authorization is called name-based authorization. · DCE. The <i>client’s DCE Extended Privilege Attribute Certificate (EPAC) is provided to the server with each remote procedure call</i> made using the binding parameter. The EPAC contains the principal name and a list of groups of which the principal is member. The EPAC also contains the name and group memberships of a principal in the delegation chain and any extended attributes that apply to the principal. <p>(Lendenmann at 193, emphasis added.)</p> <p>Lendenmann further describes how the server verifies that the client is entitled to have access to the requested remote procedure call:</p> <p>The remote procedure begins execution. It extracts the client principal name and its Extended Privilege Attribute</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>Certificates (EPACs) and <i>checks whether the client is authorized to execute the procedure</i>. If the server has implemented an ACL manager, the security information is passed to the ACL manager for evaluation of the permissions. Then the procedure executes and returns the results to the server stub, which marshalls the results and transmits them, via server’s RPC runtime, back to the client.</p> <p>(Lendenmann at 208.)</p> <p>An encrypted RPC call sent to the server with authentication and authorization information is “an access request message to the secure computer network address” as recited in the claim.</p> <p>Thus, Lendenmann teaches “sending an access request message to the secure computer network address” as recited in the claim.</p> <hr/> <p>[1.4b] <i>using a virtual private network communication link.</i></p> <p>Lendenmann teaches that the remote procedure call between the client and server is a virtual private network communication link. For example, Lendenmann teaches that the remote procedure call includes checks on the authentication of both the client and server identities and on the client’s authorization to perform the call:</p> <p>The DCE Remote Procedure Call (RPC) programming facility is connected with the security components to provide <i>mutual client/server authentication</i> of principal identity.</p> <p>(Lendenmann at 192.)</p> <p><i>Authorization is the mechanism that allows the server to control client access to a resource.</i> The authorization process is application dependent. It is up to the server side of the application to implement the appropriate authorization checking it needs. The authorization process involves the matching of clients’ privilege attributes against the permissions associated with an object.</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>The server can ask the RPC runtime for the privileges associated with a client.</p> <p>(Lendenmann at 193.)</p> <p>Lendenmann further teaches that all communications may be encrypted:</p> <p>The following protection levels are available: ... · <i>Packet Privacy</i>. Encrypts RPC arguments and data in each call using DES.</p> <p><i>Encryption is done with the session key, which is only known by the client and the server</i> for which the service ticket was issued.</p> <p>(Lendenmann at 192, emphasis added.)</p> <p>The client RPC runtime <i>encrypts the RPC call with the session key</i> and sends it to the server’s runtime together with the ticket.</p> <p>(Lendenmann at 194, emphasis added.)</p> <p>In summary, Lendenmann teaches that a remote procedure call provides communication privacy through authentication of client and server identities, authorization checks, and encryption. Thus, Lendenmann teaches that communications via a remote procedure call may be secure and private even when conducted over an insecure communication path.</p> <p>Accordingly, the authenticated, authorized, and encrypted remote procedure call is a “virtual private network communication link” under at least the broadest reasonable interpretation of that limitation.</p> <p>Lendenmann further teaches how a client can communicate securely with a server in a different cell. As Lendenmann explains, a cell is a “collection of machines, operating systems and networks.” (Lendenmann at 7.) Thus, intercell communication (or communication from one cell to another cell) is a form of <i>inter-network</i> communication. Lendenmann</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>also teaches that “access of the foreign cell is established over the Internet.” (Lendenmann at 23.) It is understood that the Internet provides an insecure communication path.</p> <p>Lendenmann teaches securing such communications between different cells and networks:</p> <p>The <i>intercell authentication process</i> is similar to the one we discussed. When a client principal wants to communicate with a foreign server principal, the client’s security runtime recognizes by the name that the server is foreign and makes a request to the local AS for a TGT to the AS of the foreign cell. This request is called a Foreign TGT (FTGT) request or Cross-Cell TGT (XTGT).</p> <p>The FTGT request proceeds like the request of any other TGT. The local AS constructs a ticket with the EPAC of the client and encrypts it using the secret key that the two authentication surrogates share. With this FTGT, the client requests a ticket to the foreign Privilege Service (PS) from the foreign AS. Because the FTGT is <i>encrypted</i> on the shared surrogate key, the foreign AS trusts the client and gives it a ticket to the foreign PS. The client then requests a Foreign PTGT (FPTGT) or Cross-Cell PTGT (XPTGT) from the foreign Privilege Service. The FPTGT is simply the client’s <i>original EPAC reencrypted</i> with the key of the foreign PS. With the FPTGT, the client can request a ticket to any principal on the foreign cell.</p> <p>If users have access to an account defined in the foreign registry, they can log in to that account by specifying the full principal name. For example, once the trust relationship is established between the two cells, a user in cell <i>itso7.austin.ibm.com</i>, with an account <i>gerardo</i> in the foreign cell <i>itso1.austin.ibm.com</i>, can log in as follows:</p> <pre># dce_login /.../itso1.austin.ibm.com/gerardo Enter Password: #</pre>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>By providing authenticated and encrypted communications between computer cells and networks over the Internet, Lendenmann teaches sending an access request message “using a virtual private network communication link” as recited in the claim.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (E.D. Tex. Opinion at 10.)</p> <p>Thus, Lendenmann teaches sending an access request message “using a virtual private network communication link” as recited in the claim.</p>
<p>[2.0] The method according to claim 1, wherein the step of receiving the secure domain name includes steps of:</p>	<p>[2.0] <i>The method according to claim 1, wherein the step of receiving the secure domain name includes steps of:</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[2.1a] receiving a command to establish the virtual private network communication link [2.1b] with a secure computer network address corresponding to a predetermined non-secure domain name; and</p>	<p>[2.1a] <i>receiving a command to establish the virtual private network communication link</i></p> <p>Lendenmann discloses receiving a command to establish a virtual private network communication link. As previously analyzed in portions [1.4a] and [1.4b], Lendenmann teaches that a remote procedure call (RPC) may include checks on authentication, authorization, and encryption, thus making the remote procedure call a “virtual private network communication link” as recited in the claim.</p> <p>Lendenmann further teaches receiving a command to establish the remote procedure call. To begin with, Lendenmann teaches that the process of establishing a remote procedure call is referred to as “binding”:</p> <p>The process of finding the server and <i>establishing a</i></p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p><i>relationship over a communication link</i> between the client and server RPC runtimes <i>is called a binding</i>. 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 import operations. A client can also obtain server binding information in string format (called string binding) from an application-specific source, such as a file or an environment variable.</p> <p>(Lendenmann at 182.)</p> <p>Lendenmann teaches that a binding includes information indicating the level of security associated with a communication link, thus indicating whether it is a virtual private network communication link:</p> <p>The binding handles are annotated with security information. The server adds the levels of security its supports to the handles registered with its RPC runtime. <i>The client adds the requested security level</i> and its own identity into the binding handle used to contact the server.</p> <p>(Lendenmann at 185.)</p> <p>Lendenmann also teaches various application programming interfaces (APIs), or routines, that receive requests to import or lookup a binding using the Cell Directory Service (CDS), as analyzed above in claim 1:</p> <p>The Name Service Interface defines several kinds of Cell Directory Service (CDS) entries that can be made in the namespace. The NSI interface provides <i>APIs which allow servers to export binding information into CDS objects and clients to import them</i>.</p> <p>...</p> <p>NSI provides two methods for finding a server, the</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>rpc_ns_binding_import_*() routines and the rpc_ns_binding_lookup_*() routines. Both operations search server entries for a compatible server.</p> <p>The difference between import and lookup operations is that the lookup operations return a list of binding handles in the sequence in which they are stored in CDS, while the former returns just one randomly chosen binding handle at a time.</p> <p>(Lendenmann at 186.)</p> <p>Finally, Lendenmann teaches that each remote procedure call on the client has a “client stub” procedure that is actually called by an application needing to invoke the remote procedure call:</p> <ol style="list-style-type: none">3. Client issues an RPC call 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 to the server. <i>The client calls the remote procedure, which actually goes to the client stub.</i> The client stub gets the arguments, marshalls them and calls the RPC runtime.4. Client’s RPC runtime requests an endpoint Binding handles obtained from CDS are usually incomplete; they lack an endpoint. The client RPC runtime must contact the endpoint mapper (dced) of the server machine. The endpoint mapper, to which all application servers register their interfaces, searches its database and returns the full binding handle for a (randomly selected) compatible server. If the client specified a fully bound handle with its RPC call, this step would not be necessary.5. Client’s RPC runtime calls the application server The client’s runtime can now make a call to the application server. <p>(Lendenmann at 208.)</p> <p>Calling the client stub initiates the remote procedure call. Thus,</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>Lendenmann teaches that the client stub “receiv[es] a command to establish the virtual private network communication link” as recited in the claim.</p> <p>[2.1b] <i>with a secure computer network address corresponding to a predetermined non-secure domain name</i></p> <p>In addition to the secure domain names analyzed in portion [1.1], Lendenmann teaches that a secure computer network address may be associated with a non-secure domain name. For example, Lendenmann teaches creating an alias, or a second name, that is an ordinary DNS name:</p> <p style="padding-left: 40px;">Cell aliasing enables cell names to be changed and allows cells to have multiple names to reflect changes in an organization. Your 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 services 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, <i>you obtain a DNS name for the cell, and set it up as a cell alias</i>. The GDS name remains the primary name.</p> <p style="padding-left: 40px;">To change the cell name, you would first assign an alias name with the following command:</p> <p style="padding-left: 80px;">dcecp> cellalias create <new_name></p> <p>(Lendenmann at 24, emphasis added.)</p> <p>Through the alias name, Lendenmann teaches that the target for a remote procedure call could alternatively be an ordinary DNS name, which is a “predetermined non-secure domain name” as recited in the claim.</p>
<p>[2.2] automatically generating a secure domain name corresponding to</p>	<p>[2.2] <i>automatically generating a secure domain name corresponding to the non-secure domain name.</i></p> <p>Lendenmann teaches that a cell can have only one name “primary” name</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>the non-secure domain name.</p>	<p>that it returns in response to inquiries. In the example of Lendenmann, the primary name is a “GDS global directory service” name:</p> <p>Your cell has a primary name, which is <i>the name that DCE services return for the cell when queried</i>, and one or more alias names that the DCE services 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. <i>The GDS name remains the primary name.</i></p> <p>(Lendenmann at 24, emphasis added.)</p> <p>Lendenmann further explains that a GDS name is in X.500 format, which as analyzed in portion [1.1] is a “secure domain name”:</p> <p>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.</p> <p>(Lendenmann at 23.)</p> <p>In summary, Lendenmann teaches that even when queried using an alternate name, such as a non-secure DNS name, a server will return its primary name that is a secure X.500 domain name.</p> <p>Thus, Lendenmann teaches “automatically generating a secure domain name corresponding to the non-secure domain name” as recited in the claim.</p>
<p>[3.0] The method according to claim 2,</p>	<p>[3.0] <i>The method according to claim 2</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 2.</p>
<p>[3.1] wherein the step of receiving a command to establish the virtual</p>	<p>[3.1] <i>wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.</i></p>

EXHIBIT E-1
Lendenmann

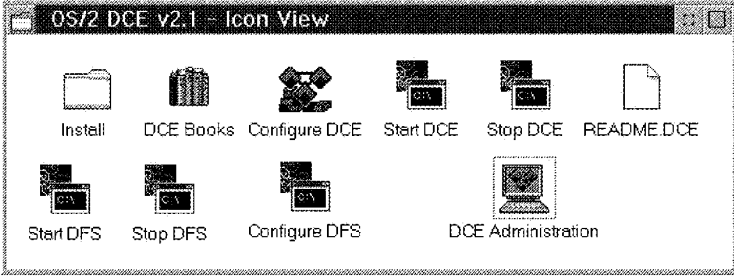
<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>private network communication link includes a step of selecting a predetermined icon displayed on a computer display.</p>	<p>Lendenmann teaches initiating a secure communications link by selecting an icon. For example, Lendenmann illustrates various program icons on a computer display in Fig. 45 (below). The program icons include an icon for “DCE Administration.”</p>  <p style="text-align: center;">Lendenmann Fig. 45</p> <p>Lendenmann describes the kinds of functions that an administrator might need to perform. In view of the sensitivity of these operations, such as editing security and access control list (ACL) information, it is understood that any communications for such operations would be accomplished via a virtual private network communication link:</p> <p style="padding-left: 40px;">When managing RPC applications, an administrator might have to do the following:</p> <ul style="list-style-type: none"> · <i>Create security registry information</i> for the server (principal, account) · Create a keytab entry with password for the server · Create namespace entries for the server’s bindings · <i>Change the ACLs of objects the server principal has to access</i> · Manage the endpoint mapper of the server’s DCE daemon <p>(Lendenmann at 202, emphasis added.)</p> <p>Lendenmann further describes a banking program that uses both the naming (via cell directory server, CDS) and security features described by Lendenmann:</p> <p style="padding-left: 40px;">Bank demo program (/usr/lpp/dce/examples/bank) — The</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>DCE Motif Bank demo is a client/server application that exploits all core services of DCE (threads, RPC, CDS, Security and DTS). An OSF/Motif front-end <i>provides a graphical user interface to operations</i> of the bank.</p> <p>(Lendenmann at 233, emphasis added.)</p> <p>Similar to the graphical user interface illustrated in Fig. 45, it is understood that the bank demo program could be started through selecting an icon on the display in the graphical user interface. Since the bank demo program uses the RPC and security features described in Lendenmann, it is further understood that using the bank demo program involves establishing a virtual private network communication link between the client and server.</p> <p>Thus, Lendenmann teaches that establishing a virtual private network communication link may include the step of “selecting a predetermined icon displayed on a computer display” as recited in the claim.</p>
<p>[4.0] The method according to claim 1,</p>	<p>[4.0] <i>The method according to claim 1</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[4.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[4.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>As analyzed above in portion [1.3], Lendenmann teaches that a cell directory server (CDS) returns a response message.</p> <p>Lendenmann further teaches that the response message includes provisioning information for the virtual private network. For example, Lendenmann teaches that the response from the cell directory server (CDS) includes an object UUID (universally unique identifier):</p> <p>When a client wants to connect to a server, it needs to find a compatible server. A server is considered compatible if it offers the same interface UUID, the same major interface version number, the same or a higher minor version number, the same protocol sequence, and the same object UUID as the</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>client requests. The requirement for the same object UUID is not so strict. If the client requests a non-nil object UUID not offered by the server, the nil object UUID is considered compatible. <i>On the other hand, if the client requests the nil object UUID, it might get a randomly selected object UUID</i> (including nil) back from CDS.</p> <p>(Lendenmann at 185.)</p> <p>Lendenmann teaches that the object UUID specifies resources used by the server:</p> <p style="padding-left: 40px;">A server may manage several distinct objects or resources within one or multiple interfaces. The purpose of object UUIDs is <i>to specify a particular object or resource the server needs to work on.</i></p> <p>(Lendenmann at 183.)</p> <p>The object UUID is “provisioning information for the virtual private network” as recited in the claim.</p> <p>And as analyzed in portion [2.1a], Lendenmann teaches that a the process of establishing a remote procedure call is known as a “binding.” Lendenmann teaches that a binding is annotated with a server’s supported security levels for each remote procedure call:</p> <p style="padding-left: 40px;">The binding handles are annotated with security information. <i>The server adds the levels of security its supports to the handles registered with its RPC runtime.</i> The client adds the requested security level and its own identity into the binding handle used to contact the server.</p> <p>(Lendenmann at 185, emphasis added.)</p> <p>The binding information specifying supported levels of security is “provisioning information for the virtual private network” as recited in the claim.</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>Thus, Lendenmann teaches “wherein the response message contains provisioning information for the virtual private network” as recited in the claim.</p>
<p>[6.0] The method according to claim 4,</p>	<p>[6.0] <i>The method according to claim 4,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 4.</p>
<p>[6.1] wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</p>	<p>[6.1] <i>wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</i></p> <p>Lendenmann teaches inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network. For example, Lendenmann teaches that a client can specify a predetermined protection level to be used in the remote procedure call (the “virtual private network communication link” as analyzed in portion [1.4b]):</p> <p style="padding-left: 40px;">When a client establishes authenticated RPC, it can <i>specify the level of protection to be applied to its communication</i> with the server. The protection level determines the degree to which client/server messages are actually encrypted. As a rule, the more restrictive the protection level, the greater the impact on performance.</p> <p>(Lendenmann at 192, emphasis added.)</p> <p style="padding-left: 40px;">The binding handles are annotated with security information. The server adds the levels of security its supports to the handles registered with its RPC runtime. <i>The client adds the requested security level</i> and its own identity into the binding handle used to contact the server.</p> <p>(Lendenmann at 185, emphasis added.)</p> <p>For the client to specify the level of protection to the server, it is understood that the client inserts into at least one data packet at least one</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>data value representing the desired protection level.</p> <p>Lendenmann further teaches details regarding the protection levels available:</p> <p style="padding-left: 40px;">The following protection levels are available:</p> <p style="padding-left: 40px;">...</p> <ul style="list-style-type: none"> · CDMF Privacy. Encrypts RPC arguments and data in each call using CDMF. · Packet Privacy. Encrypts RPC arguments and data in each call using DES. <p>(Lendenmann at 192, emphasis added.)</p> <p>Thus, Lendenmann teaches that the “CDMF Privacy” and “Packet Privacy” protection levels are associated with DES encryption and CDMF encryption, respectively. Lendenmann further teaches that these two types of encryption use different key lengths and thus provide different levels of encryption service:</p> <p style="padding-left: 40px;">The RPC communication provides different security levels, the highest being full data encryption. However, the DES algorithm (data encryption standard) internally used by DCE cannot be exported outside the U.S. in a user accessible form. This means it cannot be used for data encryption.</p> <p style="padding-left: 40px;">On the AIX and OS/2 platforms, there is a User Data Masking Facility, which is still referred to as Common Data Masking Facility or CDMF. <i>CDMF allows you to encrypt user data in RPCs using DES with a 40-bit key instead of the standard 52-bit key.</i> Since this makes the encryption weaker, it has less export restrictions from the U.S. It is a good solution for non-U.S. customers who want increased privacy, but cannot have an export license for full DES.</p> <p>(Lendenmann, at 14.)</p> <p>In summary, Lendenmann teaches that a client can specify to a server a</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>desired level of data encryption for a remote procedure call, thereby teaching “inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network” as recited in the claim.</p>
<p>[8.0] The method according to claim 4,</p>	<p>[8.0] <i>The method according to claim 4</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 4.</p>
<p>[8.1] wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</p>	<p>[8.1] <i>wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</i></p> <p>Lendenmann teaches that the remote procedure call (the “virtual private network communication link,” as analyzed in portion [1.4b]) occurs over a TCP/IP session, which uses a moving window of valid values.</p> <p>Specifically, Lendenmann teaches using transmission control protocol (TCP) for the remote procedure call:</p> <p>An RPC protocol is a communication protocol that supports the semantics of DCE RPC API and is responsible for marshalling and unmarshalling. It runs over specific combinations of transport and network protocols. DCE RPC provides two RPC protocols:</p> <ol style="list-style-type: none"> 1. Network Computing Architecture Connection-Based Protocol (NCACN) This protocol runs over a connection-oriented transport protocol, <i>such as TCP</i>. It guarantees reliability in the delivery of data, and it provides indication of a connection loss. <p>(Lendenmann at 179.)</p> <p>The transmission control protocol (TCP) is defined in RFC 793, which requires comparing a received value in a packet to a moving window of valid values:</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>The typical kinds of sequence number comparisons which the TCP must perform include:</p> <p>...</p> <p>(c) Determining that an incoming segment contains sequence numbers which are expected (i.e., that the segment "overlaps" the receive window).</p> <p>(RFC 793 at 24.)</p> <p>The first part of this test checks to see if the beginning of the segment falls in the window, the second part of the test checks to see if the end of the segment falls in the window; if the segment passes either part of the test it contains data in the window.</p> <p>(RFC 793 at 26.)</p> <p>It is understood that Lendenmann’s remote procedure call, which operates over TCP, uses “a moving window of valid values” as recited in the claim.</p>
<p>[9.0] The method according to claim 4,</p>	<p>[8.0] <i>The method according to claim 4</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 4.</p>
<p>[9.1a] wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address [9.1b] to a table of valid discriminator fields.</p>	<p>[9.1a] <i>wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address</i></p> <p>Lendenmann teaches that a virtual private network formed by a remote procedure call is based on a comparison of a discriminator field to a table of valid discriminator fields.</p> <p>Specifically, Lendenmann teaches that each remote procedure call requires not just the network address of the server, but also the “endpoint” identifier of a specific service offered by the server:</p> <p>A DCE server host may run several RPC server applications. For an RPC client to connect to a particular RPC server, it</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>needs to know the:</p> <ul style="list-style-type: none">· Network address of the server machine· Address of the process serving the call, called an endpoint <p>(Lendenmann at 188.)</p> <p>Lendenmann further teaches that in an Internet Protocol (IP) network using the TCP/IP communication protocol, the endpoint identifier is a port number:</p> <p>An endpoint is a transport-layer address to the application server. The endpoint address is specific to the transport protocol the application server will use. For example, in TCP/IP, the machine address is the IP address, and the <i>endpoint is the port address</i>. Together, they build an IP socket to which the server process is listening.</p> <p>(Lendenmann at 188, emphasis added.)</p> <p>Lendenmann also teaches that the port number is used to discriminate among multiple services offered by a server:</p> <p>As part of the RPC binding process between a client and a server, the endpoint mapper tells the client <i>which port it should use to connect to the desired server process</i>.</p> <p>(Lendenmann at 188.)</p> <p>Thus, Lendenmann teaches that the endpoint identifier (which is a port number in an IP network) is a discriminator field.</p> <p>Those of skill in the art would have understood that the port number is included in the header of every packet sent to the server. For example, the standard header for a TCP/IP packet (as defined in RFC 793) includes both the source and destination port numbers as the first two fields:</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>TCP Header Format</p> <pre> 0 1 2 3 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 ----- ----- ----- ----- Source Port Destination Port ----- ----- ----- ----- Sequence Number ----- ----- ----- ----- Acknowledgment Number ----- ----- ----- ----- Data Reserved U{A}P R{S}F Offset R{C}S{S}Y{I} Window G{K}B{T}N{N} ----- ----- ----- ----- Checksum ----- ----- ----- ----- Urgent Pointer ----- ----- ----- ----- Options Padding ----- ----- ----- ----- data ----- ----- ----- ----- </pre> <p>TCP Header Format</p> <p>(RFC 793 at 15.)</p> <p>Thus, Lendenmann teaches that the endpoint or port number is a “discriminator field in a header of each data packet to the secure computer network address” as recited in the claim.</p> <hr/> <p>[9.1b] <i>to a table of valid discriminator fields</i></p> <p>Lendenmann teaches that a secure server may offered many services through multiple different kinds of remote procedure calls, each with a distinct endpoint (or port number, as shown in portion [9.1a]):</p> <p>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.</p>

EXHIBIT E-1
Lendenmann

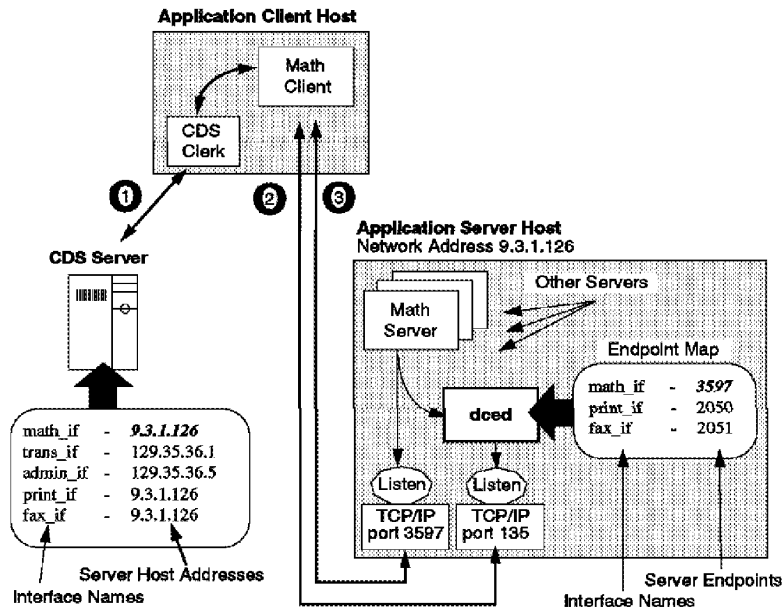
U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>(Lendenmann at 179.)</p> <p>Lendenmann further teaches that the server maintains a “system-wide list” of valid endpoints:</p> <p style="padding-left: 40px;">Server host DCE daemon (endpoint mapper) — <i>A system-wide list with</i> an entry for each combination of supported objects, interfaces, protocols, and <i>endpoints for all application servers.</i></p> <p>(Lendenmann at 182, emphasis added.)</p> <p>Lendenmann also teaches that a client can query the server to locate an appropriate endpoint for a requested service. Lendenmann teaches that the endpoint map is stored as a database:</p> <p style="padding-left: 40px;">The client selects a binding handle and issues the RPC call. Since the handle is a partly bound handle, the call goes to the remote DCE daemon listening on the well-known endpoint 135. <i>The endpoint mapper function of the DCE daemon looks up the endpoint</i> registered for the requested interface, object and protocol. It adds the endpoint to the binding handle and returns it to the client’s RPC runtime.</p> <p>(Lendenmann at 191.)</p> <p>4. Client’s RPC runtime requests an endpoint</p> <p style="padding-left: 40px;">Binding handles obtained from CDS are usually incomplete; they lack an endpoint. The client RPC runtime must contact the endpoint mapper (dced) of the server machine. <i>The endpoint mapper</i>, to which all application servers register their interfaces, <i>searches its database</i> and returns the full binding handle for a (randomly selected) compatible server. If the client specified a fully bound handle with its RPC call, this step would not be necessary.</p> <p>(Lendenmann at 208.)</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102
	<p>Finally, Lendenmann illustrates an example of displaying the endpoint map on a server:</p> <p>DCE provides several commands to manipulate the local endpoint map. To show the endpoint map on the local machine, you can use the following command:</p> <pre>dcecp> endpoint show {{object 07dfb17a-b54e-11ce-aaaa-10005a4f4629}} {interface {e1af8308-5d1f-11c9-91a4-08002b14a0fa 3.0}} {binding {ncacn_ip_tcp 9.3.1.68 135}} {annotation {Endpoint Resolution}} . . {{object 019ee420-682d-11c9-a607-08002b0dea7a}} {interface {019ee420-682d-11c9-a607-08002b0dea7a 1.0}} {binding {ncadg_ip_udp 9.3.1.68 1204}} {annotation {Time Service}}</pre> <p>(Lendenmann at 205.)</p> <p>Lendenmann also provides an example illustration of an endpoint map as a two-column table on the right side of Fig. 68:</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180* Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102



Lendenmann Fig. 68 (at 190)

Thus, Lendenmann’s endpoint map is a “table of valid discriminator fields” as recited in the claim.

Lendenmann also teaches that when a remote procedure call arrives at a server, the server consults an entry point vector (EPV) table to determine the appropriate function to perform the requested remote procedure call:

When a call arrives at the server, the server must be able to determine which routine to call. The manager is part of the server implementation that contains all procedures defined in the interface.

For each interface supported by the server, there is an entry-point vector (EPV) that contains a list of addresses of the remote procedures provided by the manager. It is an array of function pointers. A manager EPV must contain exactly one entry point for each procedure defined in the interface

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>definition. A default manager EPV is typically generated into the stub code by the IDL compiler. A server that does not handle several managers can use the default EPV provided in the stub.</p> <p>(Lendenmann at 189.)</p> <p>Thus, the entry point vector (EPV) is also a “table of valid discriminator fields” as recited in the claim.</p> <p>Accordingly, Lendenmann teaches that “the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields” as recited in the claim.</p>
<p>[10.0] The method according to claim 1,</p>	<p>[10.0] <i>The method according to claim 1,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[10.1] wherein the virtual private network includes the Internet.</p>	<p>[10.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>Lendenmann teaches that the virtual private network includes the Internet. For example, Lendenmann teaches that communications between a first network (cell) and a second network (foreign cell) occur via the Internet:</p> <p>The only well-established, multi-vendor-supported global network today is the Internet. It has global addressing and routing. The DNS naming scheme makes direct use of the Internet naming and routing scheme by extending the information that each Internet DNS server carries. 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. So, <i>the access of the foreign cell is established over the Internet</i> in both cases.</p> <p>(Lendenmann at 23, emphasis added.)</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>Lendenmann provides a specific example in Fig. 12 of communications between an “ibm.com” cell and an “osf.org” cell. The two cells use the Internet Domain Name Service (DNS) to locate each others’ network addresses. It is understood that DNS returns Internet addresses, and thus the communications between the cells occurs via the Internet:</p> <div data-bbox="516 772 1344 1129" data-label="Diagram"> </div> <p style="text-align: center;">Lendenmann Fig. 12 (at 25)</p> <p>More generally, Lendenmann teaches that the remote procedure call (which establishes the virtual private network) uses a set of protocols based on the Internet Protocol (IP) that is used for communications over the Internet:</p> <p style="padding-left: 40px;">An example of a protocol set is the Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Protocol (IP), commonly known as TCP/IP. IP implements the network layer of the OSI model. TCP and UDP implement the transport protocol, which both use IP.</p> <p>(Lendenmann at 179.)</p> <p>Thus, Lendenmann teaches that “the virtual private network includes the Internet” as recited in the claim.</p>
<p>[12.0] The method according to claim</p>	<p>[12.0] <i>The method according to claim 1,</i></p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>1,</p>	<p>As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[12.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[12.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i></p> <p>Lendenmann teaches that the access request message contains a request for information stored at the secure computer network address. For example, Lendenmann teaches a Distributed File System (DFS) service that builds on the remote procedure call (RPC) architecture analyzed above in claim 1:</p> <p style="padding-left: 40px;">The Distributed File System (DFS) presents directories and files in a global namespace that can be accessed from any DFS client...</p> <p style="padding-left: 40px;">The DFS is built on top of the core technologies: Security Service, Cell Directory Service and Distributed Time Service. <i>DFS also makes use of threads and RPCs.</i></p> <p>(Lendenmann at 11, emphasis added.)</p> <p>Lendenmann illustrates clients submitted requests for information stored at a secure server in Fig. 35:</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<div data-bbox="552 514 1299 1060" data-label="Diagram"> <p>The diagram illustrates the DFS architecture. On the left, a dashed box labeled 'DFS Server' contains a computer icon and a 'File Exporter' oval. A central cloud-like shape represents the 'Network'. On the right, two dashed boxes represent 'DFS Client' units. Each DFS Client contains a computer icon, a 'Client Appl.' oval, and a 'Cache Manager' oval. Arrows show the 'File Exporter' connected to the 'Network', and the 'Network' connected to the 'Client Appl.' of each DFS Client. Dashed arrows also point from the 'Client Appl.' to the 'Cache Manager' within each client.</p> </div> <p style="text-align: center;">Lendenmann Fig. 35 (at 98)</p> <p>Lendenmann also explains how the clients access files using a remote procedure call (RPC), which is an “access request message” as analyzed above in portion [1.4a]:</p> <p style="padding-left: 40px;">There may be many DFS file servers in a cell. Each DFS file server runs <i>the file exporter service which makes files available to DFS clients</i>. The file exporter is also known as the protocol exporter .</p> <p style="padding-left: 40px;">DFS clients run the cache manager, an intermediary between applications that requests files from DFS servers. The cache manager <i>translates file requests into RPCs to the file exporter on the file server system</i> and stores (caches) file data on disk or in memory to minimize server accesses. It also ensures that the client always has an up-to-date copy of a file.</p> <p>(Lendenmann at 98.)</p> <p>It is understood that files served by the file exporter service on the DFS</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>file server are “information.” Since the file requests are transmitted to the DFS file server using remote procedure calls (RPCs) (which as analyzed at portion [1.4b] may be encrypted), the DFS file server is at a secure computer network address.</p> <p>Thus, Lendenmann teaches “wherein the access request message contains a request for information stored at the secure computer network address” as recited in the claim.</p>
<p>[13.0] The method of claim 1,</p>	<p>[13.0] <i>The method of claim 1,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[13.1] wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>[13.1] <i>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</i></p> <p>As analyzed in portion [1.1], Lendenmann illustrates in Fig. 15 that a CDS clerk—executing on the same computer as a client application—receives the secure domain name:</p> <p>Figure 15 shows the look-up process:</p> <ol style="list-style-type: none"> 1. The client application on node 1 sends a look-up request to the local clerk. <p>...</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180* Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102

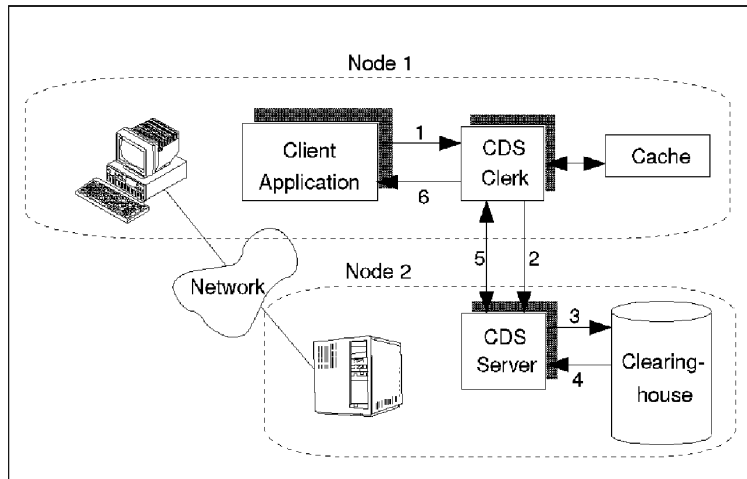


Figure 15. CDS Components Performing a CDS Look-up

(Lendenmann at 29-30.)

Thus, Lendenmann’s node 1 that executes the CDS clerk and client application is a “client computer.”

Lendenmann further teaches that the secure domain name is provided by a user:

The directory service is the process that *makes it possible for the user to locate objects* in the network without knowing their physical location. It hides from the user the distributed nature of the environment. It is like a telephone directory assistance service that provides the phone number when given a person’s name.

Users do not normally access or use the directory services directly. They run applications which might use the directory services to find objects. *The only thing a user might have to know is object names* and maybe the naming model.

(Lendenmann at 19, emphasis added.)

DCE Naming Service provides a naming model throughout

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>the distributed environment. This model <i>allows users to identify, by name, resources, such as servers</i>, files, disks, or print queues, and gain access to them without needing to know where they are located in a network. Further, <i>users can continue referring to a resource by the same name</i> even when a characteristic of the resource changes, such as its network address.</p> <p>(Lendenmann at 22, emphasis added.)</p> <p>Thus, Lendenmann teaches “wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user” as recited in the claim.</p>
<p>[13.2] wherein sending the query message comprises sending the query message at the client computer;</p>	<p>[13.2] <i>wherein sending the query message comprises sending the query message at the client computer;</i></p> <p>As analyzed above in portion [13.1], Lendenmann illustrates an example of a client computer as node 1 in Fig. 15. And as analyzed in portion [1.2], Lendenmann teaches that the CDS clerk on node 1 sends the query message to a server:</p> <ol style="list-style-type: none"> 2. The clerk checks its cache and, not finding the name there, contacts the server on node 2. <p>...</p>

EXHIBIT E-1
Lendenmann

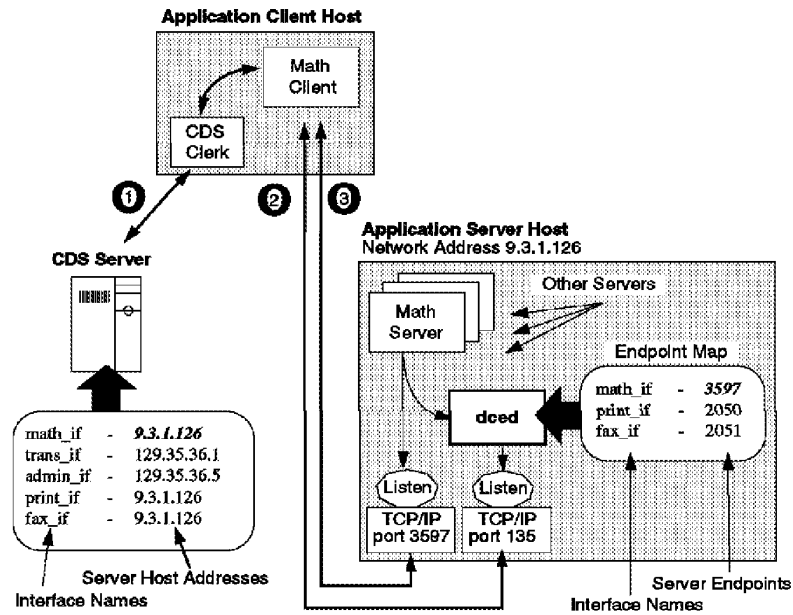
<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<div data-bbox="565 527 1312 995" data-label="Diagram"> </div> <p data-bbox="565 1003 1031 1024">Figure 15. CDS Components Performing a CDS Look-up</p> <p data-bbox="505 1062 786 1094">(Lendenmann at 29-30.)</p> <p data-bbox="505 1129 1360 1224">Thus, Lendenmann teaches “wherein sending the query message comprises sending the query message at the client computer” as recited in the claim.</p>
<p>[13.3] wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p data-bbox="505 1266 1333 1329">[13.3] wherein receiving the response message comprises receiving the response message at the client computer,</p> <p data-bbox="505 1362 1349 1493">As analyzed above in portion [13.1], Lendenmann illustrates an example of a client computer as node 1 in Fig. 15. And as analyzed in portion [1.3], Lendenmann teaches that the CDS clerk on node 1 receives the response message:</p> <p data-bbox="574 1528 1008 1560">Figure 15 shows the look-up process:</p> <p data-bbox="574 1575 602 1596">...</p> <p data-bbox="574 1598 1295 1661">5. <i>The server returns the information to the clerk</i> on node 1.</p> <p data-bbox="574 1675 602 1696">...</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<div data-bbox="565 527 1312 995" data-label="Diagram"> </div> <p data-bbox="565 1003 1036 1024">Figure 15. CDS Components Performing a CDS Look-up</p> <p data-bbox="505 1062 987 1094">(Lendenmann at 29-30, emphasis added.)</p> <p data-bbox="505 1129 1312 1224">Thus, Lendenmann teaches “wherein receiving the response message comprises receiving the response message at the client computer” as recited in the claim.</p>
<p>[13.4] wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p data-bbox="505 1266 1369 1329">[13.4] wherein sending the access request message comprises sending the access request message at the client computer.</p> <p data-bbox="505 1365 1339 1560">As analyzed in portion [1.4a], Lendenmann teaches sending the access request message from a client. Lendenmann illustrates, for example in Fig. 68, an Application Client Host computer running a math client and the CDS clerk. The Application Client Host corresponds to the client computer running the client application and CDS clerk analyzed in portion [13.1]:</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180* Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102



Lendenmann Fig. 68 (at 190)

As illustrated in Fig. 68, the client computer sends an access request message to an Application Server Host.

Thus, Lendenmann teaches sending the access request message from the same “client computer” previously identified and analyzed in portion [13.1].

Thus, Lendenmann teaches “wherein sending the access request message comprises sending the access request message at the client computer” as recited in the claim.

<p>[14.0] The method of claim 1,</p>	<p>[14.0] <i>The method of claim 1,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[14.1] performed by a software module.</p>	<p>[14.1] <i>performed by a software module.</i> Lendenmann teaches that the method of claim 1 may be performed by a</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>software module. All of the steps analyzed above with respect to claim 1 are performed by a software module.</p> <p>For example, Lendenmann illustrates the various components of the Distributed Computing Environment (DCE) software module:</p> <div data-bbox="639 730 1230 1264" data-label="Diagram"> </div> <p style="text-align: center;">Lendenmann Fig. 3 (at 8)</p> <p>Thus, Lendenmann teaches the method of claim 1 “performed by a software module” as recited in the claim.</p>
<p>[15.0] The method of claim 1,</p>	<p>[15.0] <i>The method of claim 1,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 1.</p>
<p>[15.1] performed by a client computer.</p>	<p>[15.1] <i>performed by a client computer.</i> See analysis of claim 13. Lendenmann teaches that all of the steps of claim 1 are performed by a client computer such as “node 1” in Fig. 15 or the Application Client Host of Fig. 68.</p>
<p>[16.0] The method</p>	<p>[16.0] <i>The method of claim 2</i></p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>of claim 2,</p>	<p>As analyzed above, Lendenmann teaches all of the limitations of claim 2.</p>
<p>[16.1] wherein receiving the command comprises receiving the command at a client computer from a user.</p>	<p>[16.1] <i>wherein receiving the command comprises receiving the command at a client computer from a user.</i></p> <p>As shown in the analysis of portion [13.1], Lendenmann teaches receiving the secure domain name from a user. Lendenmann further teaches that the command to establish a virtual private network communication link comes from a user. For example, as analyzed in portion [12.1], Lendenmann teaches that a user may access files from a distributed file service:</p> <p style="padding-left: 40px;">The Distributed File Service (DFS) is a DCE application that provides global file sharing. <i>Access to files located anywhere in interconnected DCE cells is transparent to the user.</i> To the user, it appears as if the files were located on a local drive.</p> <p>(Lendenmann at 97, emphasis added.)</p> <p>And as analyzed in portions [12.1] and [1.4b], Lendenmann teaches that access to the distributed file service is through a remote procedure call that forms a virtual private network communication link.</p> <p>Thus, Lendenmann teaches “wherein receiving the command comprises receiving the command at a client computer from a user” as recited in the claim.</p>
<p>[17.0] A computer-readable storage medium, comprising:</p>	<p>[17.0] <i>A computer-readable storage medium, comprising:</i></p> <p>Lendenmann discloses a computer-readable storage medium. For example, Lendenmann describes installing from an input device the DCE software that includes the remote procedure call (RPC), cell directory service (CDS), and distributed file system (DFS) analyzed throughout this claim chart:</p> <p style="padding-left: 40px;">Installation is done using smit or the installp command. To install DCE call smit in the following way:</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1-4, 6, 8-10, 12-20, 22, 24-26, 28-35, 37, and 39-40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>																																	
	<pre># smitty installp ->Install/Update From All Available Software Select your input device, and then you'll get:</pre> <div data-bbox="597 716 1317 1192" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">Install/Update From All Available Software</p> <p>Type or select values in entry fields. Press Enter AFTER making all desired changes.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">* INPUT device / directory for software</td> <td style="width: 20%;">[Entry Fields]</td> <td style="width: 20%;"></td> </tr> <tr> <td>* SOFTWARE to install</td> <td>/dev/rmt0.1</td> <td style="text-align: right;">+</td> </tr> <tr> <td>PREVIEW only? {install operation will NOT occur}</td> <td><input type="checkbox"/></td> <td style="text-align: right;">+</td> </tr> <tr> <td>COMMIT software updates?</td> <td>no</td> <td style="text-align: right;">+</td> </tr> <tr> <td>SAVE replaced files?</td> <td>yes</td> <td style="text-align: right;">+</td> </tr> <tr> <td>ALTERNATE save directory</td> <td><input type="checkbox"/></td> <td style="text-align: right;">+</td> </tr> <tr> <td>AUTOMATICALLY install requisite software?</td> <td>yes</td> <td style="text-align: right;">+</td> </tr> <tr> <td>EXTEND file systems if space needed?</td> <td>yes</td> <td style="text-align: right;">+</td> </tr> <tr> <td>OVERWRITE same or newer versions?</td> <td>no</td> <td style="text-align: right;">+</td> </tr> <tr> <td>VERIFY install and check file sizes?</td> <td>no</td> <td style="text-align: right;">+</td> </tr> <tr> <td>DETAILED output?</td> <td>no</td> <td style="text-align: right;">+</td> </tr> </table> <p style="font-size: small; margin-top: 10px;"> F1=Help F2=Refresh F3=Cancel F4=List F5=Reset F6=Command F7=Edit F8=Image F9=Shell F10=Exit Enter=Do </p> </div> <p>(Lendenmann at 104-05, annotated.)</p> <p>The “INPUT device / directory for software” is a computer-readable storage medium.</p> <p>Lendenmann further teaches that the DCE software may be installed, for example, to a “C:” drive, as illustrated in Fig. 42:</p>	* INPUT device / directory for software	[Entry Fields]		* SOFTWARE to install	/dev/rmt0.1	+	PREVIEW only? {install operation will NOT occur}	<input type="checkbox"/>	+	COMMIT software updates?	no	+	SAVE replaced files?	yes	+	ALTERNATE save directory	<input type="checkbox"/>	+	AUTOMATICALLY install requisite software?	yes	+	EXTEND file systems if space needed?	yes	+	OVERWRITE same or newer versions?	no	+	VERIFY install and check file sizes?	no	+	DETAILED output?	no	+
* INPUT device / directory for software	[Entry Fields]																																	
* SOFTWARE to install	/dev/rmt0.1	+																																
PREVIEW only? {install operation will NOT occur}	<input type="checkbox"/>	+																																
COMMIT software updates?	no	+																																
SAVE replaced files?	yes	+																																
ALTERNATE save directory	<input type="checkbox"/>	+																																
AUTOMATICALLY install requisite software?	yes	+																																
EXTEND file systems if space needed?	yes	+																																
OVERWRITE same or newer versions?	no	+																																
VERIFY install and check file sizes?	no	+																																
DETAILED output?	no	+																																

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<div data-bbox="618 522 1247 1062" data-label="Image"> </div> <p>The “C:” drive of a computer is a “computer-readable storage medium.”</p> <p>Thus, Lendenmann teaches a “computer-readable storage medium” as recited in the claim.</p>
<p>[17.1] a storage area; and</p>	<p>[17.1] a storage area; and</p> <p>See analysis of portion [17.0]. The computer-readable <i>storage medium</i> includes a “storage area.”</p> <p>For example, Lendenmann teaches that DCE may be installed to a specific directory on the target drive:</p> <p style="padding-left: 40px;">The Install — progress window will be displayed. The files are now copied from the installation media into the <i>/opt/dcelocal directory on the target drive.</i></p> <p>(Lendenmann at 118, emphasis added.)</p> <p>The “/opt/dcelocal” directory is a storage area on the computer-readable storage medium, such as the “C:” drive as analyzed in portion [17.0].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>Thus, Lendenmann teaches “a storage area” as recited in the claim.</p>
<p>[17.2] computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>[17.2] <i>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</i></p> <p>See analysis of portion [1.0]. It is understood that the DCE software system as taught by Lendenmann includes “computer-readable instructions” as recited in the claim.</p>
<p>[17.3] receiving a secure domain name;</p>	<p>[17.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[17.4] sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[17.4] <i>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>
<p>[17.5] receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>[17.5] <i>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>[17.6] sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>[17.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
<p>[18.0] The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:</p>	<p>[18.0] <i>The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 17.</p>
<p>[18.1] receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and</p>	<p>[18.1] <i>receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and</i></p> <p>See analysis of portions [2.1a]–[2.1b].</p>
<p>[18.2] automatically generating a secure domain name corresponding to the non-secure domain name.</p>	<p>[18.2] <i>automatically generating a secure domain name corresponding to the non-secure domain name.</i></p> <p>See analysis of portion [2.2].</p>
<p>[19.0] The computer-readable</p>	<p>[19.0] <i>The computer-readable medium according to claim 18,</i></p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>medium according to claim 18,</p>	<p>As analyzed above, Lendenmann teaches all of the limitations of claim 18.</p>
<p>[19.1] wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.</p>	<p>[19.1] <i>wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.</i></p> <p>See analysis of portion [3.1].</p>
<p>[20.0] The computer-readable medium according to claim 17,</p>	<p>[20.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 17.</p>
<p>[20.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[20.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>See analysis of portion [4.1].</p>
<p>[22.0] The computer-readable medium according to claim 20,</p>	<p>[22.0] <i>The computer-readable medium according to claim 20,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 20.</p>
<p>[22.1] wherein the virtual private network is based on inserting into at least one data packet at least one</p>	<p>[22.1] <i>wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</i></p> <p>See analysis of portion [6.1].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>data value representing a predetermined level of service associated with the virtual private network.</p>	
<p>[24.0] The computer-readable medium according to claim 20,</p>	<p>[24.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 20.</p>
<p>[24.1] wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</p>	<p>[24.1] <i>wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</i> See analysis of portion [8.1].</p>
<p>[25.0] The computer-readable medium according to claim 20,</p>	<p>[25.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 20.</p>
<p>[25.1] wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid</p>	<p>[25.1] <i>wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.</i> See analysis of portions [9.1a]–[9.1b].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>discriminator fields.</p>	
<p>[26.0] The computer-readable medium according to claim 17,</p>	<p>[26.0] <i>The computer-readable medium according to claim 17,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 17.</p>
<p>[26.1] wherein the virtual private network includes the Internet.</p>	<p>[26.1] <i>wherein the virtual private network includes the Internet.</i> See analysis of portion [10.1].</p>
<p>[28.0] The computer readable medium of claim 17,</p>	<p>[28.0] <i>The computer readable medium of claim 17,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 17.</p>
<p>[28.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[28.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i> See analysis of portion [12.1].</p>
<p>[29.0] The computer-readable medium according to claim 17,</p>	<p>[29.0] <i>The computer-readable medium according to claim 17,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 17.</p>
<p>[29.1] wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a</p>	<p>[29.1] <i>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</i> See analysis of portion [13.1].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>user;</p>	
<p>[29.2] wherein sending the query message comprises sending the query message at the client computer;</p>	<p>[29.2] <i>wherein sending the query message comprises sending the query message at the client computer;</i></p> <p>See analysis of portion [13.2].</p>
<p>[29.3] wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>[29.3] <i>wherein receiving the response message comprises receiving the response message at the client computer,</i></p> <p>See analysis of portion [13.3].</p>
<p>[29.4] wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>[29.4] <i>wherein sending the access request message comprises sending the access request message at the client computer.</i></p> <p>See analysis of portion [13.4].</p>
<p>[30.0] The computer-readable medium according to claim 17,</p>	<p>[30.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 20.</p>
<p>[30.1] wherein the method is performed by a software module.</p>	<p>[30.1] <i>wherein the method is performed by a software module.</i></p> <p>See analysis of portion [14.1].</p>
<p>[31.0] The computer-readable medium according to claim 17,</p>	<p>[31.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 17.</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>[31.1] wherein the method is performed by a client computer.</p>	<p>[31.1] <i>wherein the method is performed by a client computer.</i></p> <p>See analysis of portion [15.1].</p>
<p>[32.0] The computer-readable medium according to claim 18,</p>	<p>[32.0] <i>The computer-readable medium according to claim 18,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 18.</p>
<p>[32.1] wherein receiving the command comprises receiving the command at a client computer from a user.</p>	<p>[32.1] <i>wherein receiving the command comprises receiving the command at a client computer from a user.</i></p> <p>See analysis of portion [16.1].</p>
<p>[33.0] A data processing apparatus, comprising:</p>	<p>[33.0] <i>A data processing apparatus, comprising:</i></p> <p>See analysis of portions [1.0] and [17.0]. Lendenmann teaches installing and using the DCE software system on a computer. A computer is a “data processing apparatus.”</p> <p>Thus, Lendenmann teaches a “data processing apparatus” as recited in the claim.</p>
<p>[33.1] a processor, and</p>	<p>[33.1] <i>a processor, and</i></p> <p>As analyzed in portion [33.0], Lendenmann teaches installing and using the DCE software system on a computer. A computer includes a processor. For example, Lendenmann discloses using DCE software system on a computer with an Intel 386 processor:</p> <p style="padding-left: 40px;">IBM DCE for Windows runs on <i>any Intel platform with a 386 processor</i> or higher, at least 4 MB of memory, 5 MB of free disk space, and 5 MB of Windows swapfile. It requires DOS 5.0 or higher and Windows 3.1.</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
	<p>(Lendenmann at 17, emphasis added.)</p> <p>Thus, Lendenmann teaches a “processor” as recited in the claim.</p>
<p>[33.2] memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>[33.2] <i>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</i></p> <p>See analysis of portions [1.0], [17.0] and [17.1].</p> <p>As analyzed in those portions, Lendenmann teaches installing the DCE software system from an input device and to a directory on a target drive. The input device, directory, and target drive are each a “memory storing computer executable instructions,” as recited in the claim.</p> <p>As analyze in portion [1.0], Lendenmann teaches that the DCE software system enables a computer to “perform a method for accessing a secure computer network address,” as recited in the claim.</p>
<p>[33.3] receiving a secure domain name;</p>	<p>[33.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[33.4] sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[33.4] <i>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>[33.5] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p><i>[33.5] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>
<p>[33.6] sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p><i>[33.6] sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
<p>[34.0] The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:</p>	<p><i>[34.0] The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 33.</p>
<p>[34.1] receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-</p>	<p><i>[34.1] receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-</i></p> <p>See analysis of portions [2.1a]–[2.1b].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>secure domain name; and</p>	
<p>[34.2] automatically generating a secure domain name corresponding to the non-secure domain name.</p>	<p>[34.2] <i>automatically generating a secure domain name corresponding to the non-secure domain name.</i></p> <p>See analysis of portion [2.2].</p>
<p>[35.0] The apparatus of claim 33,</p>	<p>[35.0] <i>The apparatus of claim 33,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 33.</p>
<p>[35.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[35.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>See analysis of portion [4.1].</p>
<p>[37.0] The apparatus of claim 35,</p>	<p>[37.0] <i>The apparatus of claim 35,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 35.</p>
<p>[37.1] wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the</p>	<p>[37.1] <i>wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the</i></p> <p>See analysis of portion [6.1].</p>

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.1: Claims 1–4, 6, 8–10, 12–20, 22, 24–26, 28–35, 37, and 39–40 are anticipated by Lendenmann under 35 U.S.C. § 102</p>
<p>virtual private network.</p>	
<p>[39.0] The apparatus of claim 35,</p>	<p>[39.0] <i>The apparatus of claim 35,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 35.</p>
<p>[39.1] wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</p>	<p>[39.1] <i>wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</i> See analysis of portion [8.1].</p>
<p>[40.0] The apparatus of claim 35,</p>	<p>[40.0] <i>The apparatus of claim 35,</i></p>
<p>[40.1] wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.</p>	<p>[40.1] <i>wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.</i> See analysis of portions [9.1a]–[9.1b].</p>

EXHIBIT E-1
Lendenmann

Section 2 – Obviousness

Chart E-1.2: Detailed support for Proposed Rejection #2, showing that claims 5, 21, and 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103.

Bruce Schneier, APPLIED CRYPTOGRAPHY (1996).

Schneier is a printed publication publicly available more than one year before the '180 patent's earliest claimed priority date and is prior art under at least 35 U.S.C. § 102(b). A copy of Schneier is attached as Exhibit D-5.

Reasons to Combine Lendenmann and Schneier

As shown in the following analysis, Lendenmann and Schneier together teach all of the limitations of claims 5, 21, and 36. Thus, there are no substantive differences between the features taught by the prior art and the limitations recited in claims 5, 21, and 36. Accordingly, it would have been well within the ability of a person of ordinary skill in the art to combine the features of Lendenmann and Schneier.

As shown in the analysis of Lendenmann above in Section 1 – Anticipation, Lendenmann generally discloses a network architecture for secure network communications, including protections against interception by transparently encrypting packets. Schneier generally describes encryption techniques useful for protecting communications. Thus, Lendenmann and Schneier are both directed to encryption technologies used for communications.

It would have been obvious to one of skill in the art, before the filing of the '180 patent, to combine the Lendenmann network architecture with the additional techniques disclosed in Schneier because the combination is merely the use of known techniques (as shown in Schneier) to improve encryption in the Lendenmann system in the same way that these known techniques improve encryption in Schneier's examples. For example, with respect to claim 5, combining the DES encryption of Lendenmann with the random padding bits as taught by Schneier would allow Lendenmann's DES encryption scheme to operate on data with an arbitrary length. Thus, the combination would further improve the utility of Lendenmann's remote procedure call.

Additionally, it would have been obvious to combine Lendenmann and Schneier because the combination of known elements accordingly to known methods merely produces a predictable result. For example, with respect to claim 5, combining DES block encryption technique of Lendenmann with random padding bits as taught by Schneier results in the predictable result of a DES encryption technique that can operate on data with an arbitrary length. Those of skill in the art would have recognized that this predictable benefit would be available by incorporating random padding bits into Lendenmann's DES encryption technique in the way suggested by Schneier.

EXHIBIT E-1
Lendenmann

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.2: Claims 5, 21, & 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103</p>
<p>[5.0] The method according to claim 4,</p>	<p>[5.0] <i>The method according to claim 4,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 4.</p>
<p>[5.1] wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address,</p>	<p>[5.1] <i>wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address,</i> Lendenmann teaches inserting a data value into each data packet sent to the secure computer network address: 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. As a rule, the more restrictive the protection level, the greater the impact on performance. The following protection levels are available: ... · Packet. <i>Attaches a verifier to each message</i> sent over the network to make sure all messages are from the expected client. (Lendenmann at 192, emphasis added.) The verifier attached to each message is a data value inserted into each data packet. As the quoted portion of Lendenmann above explains, the verifier forms part of the protection mechanism of the secure remote procedure call (RPC). Thus, Lendenmann teaches that the remote procedure call is based in part on inserting the verifier into each message. And as analyzed above in portions [1.0] and [6.1], Lendenmann teaches</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.2: Claims 5, 21, & 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103
	<p>encrypting data packets using the DES encryption standard. Schneier teaches that the DES encryption technique is a block cipher requiring equally-sized input blocks of data. To ensure that data of any size can be encrypted, padding data is appended to make the last block a complete block of data:</p> <p style="padding-left: 40px;">DES is a block cipher; it encrypts data in 64-bit blocks.</p> <p>(Schneier at 270.)</p> <p style="padding-left: 40px;">Most messages don't divide neatly into 64-bit (or whatever size) encryption blocks; there is usually a short block at the end. ... Padding is the way to deal with this problem.</p> <p style="padding-left: 40px;">Pad the last block with some regular pattern—zeros, ones, alternating ones and zeros—to make it a complete block.</p> <p>(Schneier at 190.)</p> <p>The padding bits added in accordance with Schneier's teachings are "one or more data values" inserted into each data packet, as recited in the claim.</p> <p>Accordingly, Lendenmann teaches "wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address" as recited in the claim.</p>
<p>[5.2] the one or more data values varying according to a pseudo-random sequence.</p>	<p>[5.2] <i>the one or more data values varying according to a pseudo-random sequence.</i></p> <p>As analyzed in portion [5.1], Schneier teaches inserting padding bits that are the "data values" of the claim. Schneier teaches that the padding bits may be random:</p> <p style="padding-left: 40px;">One simple method is to add a bit of padding. <i>Pad the text with a string of random bits</i>, half a block in length, between the first and second and between the second and third encryptions.</p> <p>(Schneier at 362, emphasis added.)</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.2: Claims 5, 21, & 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103
	<p>It is understood that random bits of data used for padding on a computer would be generated using a pseudo-random sequence:</p> <p style="padding-left: 40px;">The best a computer can produce is a pseudo-random-sequence generator.</p> <p>(Schneier at 44.)</p> <p>Thus, Lendenmann in view of Schneier teaches that “the one or more data values varying according to a pseudo-random sequence” as recited in the claim.</p>
[21.0] The computer-readable medium according to claim 20,	<p>[21.0] <i>The computer-readable medium according to claim 20,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 20.</p>
[21.1] wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.	<p>[21.1] <i>wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.</i></p> <p>See analysis of portions [5.1]–[5.2].</p>
[36.0] The apparatus of claim 35,	<p>[36.0] <i>The apparatus of claim 35,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 33.</p>
[36.1] wherein the virtual private network is based on	<p>[36.1] <i>wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a</i></p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.2: Claims 5, 21, & 36 are obvious over Lendenmann in view of Schneier under 35 U.S.C. § 103
inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.	<i>pseudo-random sequence.</i> See analysis of portions [5.1]–[5.2].

EXHIBIT E-1
Lendenmann

Chart E-1.3: Detailed support for Proposed Rejection #3, showing that claims 7, 23, and 38 are obvious over Lendenmann in view of Martin under 35 U.S.C. § 103.

David M. Martin, “A Framework for Local Anonymity in the Internet,” Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998) (“Martin”).

Martin is a printed publication published before the ’180 Patent’s earliest priority date of Oct. 30, 1998 and is at least prior art under 35 U.S.C. § 102(a). Martin is attached as Exhibit D-4.

Reasons to Combine Lendenmann and Martin

As shown in the following analysis, Lendenmann and Martin together teach all of the limitations of claims 7, 23, and 38. Thus, there are no substantive differences between the features taught by the prior art and the limitations recited in claims 7, 23, and 38. Accordingly, it would have been well within the ability of a person of ordinary skill in the art to combine the features of Lendenmann and Martin.

As shown in the analysis of Lendenmann above in Section 1 – Anticipation, Lendenmann generally discloses a network architecture for secure network communications, including protections against interception by encrypting communications between a client and server. Martin generally discloses a network architecture for securing network communications against interception by routing communications through a series of randomly selected intermediaries. Thus, Lendenmann and Martin are directed to similar network security architectures and technologies.

It would have been obvious to one of skill in the art, before the filing of the ’180 patent, to combine the Lendenmann network architecture with the additional techniques disclosed in Martin because the combination is merely the use of known techniques (as shown in Martin) to improve the similar Lendenmann system in the same way that these known techniques improve the Martin system. For example, with respect to claim 7, combining the communication encryption of Lendenmann with the randomly chosen network addresses as taught by Martin would allow the Lendenmann network to prevent eavesdroppers from seeing not only the content of communications between two parties, but also *who* those parties were. Thus, the combination would further improve the security of Lendenmann’s remote procedure call.

Additionally, it would have been obvious to combine Lendenmann and Martin because the combination of known elements accordingly to known methods merely produces a predictable result. For example, with respect to claim 7, combining the encrypted remote procedure call of Lendenmann with the anonymized network addresses as taught by Martin results in the predictable result of a network that provides encrypted communications services over a network between anonymized endpoint addresses. Those of skill in the art would have recognized that

EXHIBIT E-1
Lendenmann

this predictable benefit would be available by incorporating indirect connection addressing into Lendenmann’s remote procedure call architecture in the way suggested by Martin.

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-1.3: Claims 7, 23 and 38 are obvious over Lendenmann in view of Martin under 35 U.S.C. § 103</p>
<p>[7.0] The method according to claim 4,</p>	<p>[7.0] <i>The method according to claim 4</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 4.</p>
<p>[7.1] wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</p>	<p>[7.1] <i>wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</i></p> <p>Martin teaches establishing the virtual private network communication link by creating an network address hopping regime between a first computer and a second computer:</p> <p style="padding-left: 40px;">Let A_{IP} be the set of anonymous IP addresses in the lanon, $PORT = \{0,1, \dots, 2^{16} - 1\}$ be the set of possible port numbers, and $A_{TCP} = A_{IP} \times PORT$ be the set of all possible TCP endpoint connection identifiers. Each such identifier is called an <i>anonymous TCP address</i>. A lanon client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random subject to lanon uniqueness and application-specific constraints. Randomly choosing the source label hides the node's identity from external (and internal) observers.</p> <p>(Martin at 9.)</p> <p>Choosing one of the source addresses “at random” shows establishing the virtual private network communication link through pseudorandomly changing computer network addresses as recited by the</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.3: Claims 7, 23 and 38 are obvious over Lendenmann in view of Martin under 35 U.S.C. § 103
	<p>claim.</p> <p>One of skill in the art would have been motivated to combine Martin's IP hopping scheme with Lendenmann's secure remote procedure call in order to obfuscate a client computer's network location, as described in Martin.</p>
<p>[23.0] The computer-readable medium according to claim 20,</p>	<p>[23.0] <i>The computer-readable medium according to claim 20,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 20.</p>
<p>[23.1] wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</p>	<p>[23.1] <i>wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</i></p> <p>See analysis of portion [7.1].</p>
<p>[38.0] The apparatus of claim 35,</p>	<p>[38.0] <i>The apparatus of claim 35,</i></p> <p>As analyzed above, Lendenmann teaches all of the limitations of claim 35.</p>
<p>[38.1] wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in</p>	<p>[38.1] <i>wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</i></p> <p>See analysis of portion [7.1].</p>

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.3: Claims 7, 23 and 38 are obvious over Lendenmann in view of Martin under 35 U.S.C. § 103
packets transmitted between a first computer and a second computer.	

EXHIBIT E-1
Lendenmann

Chart E-1.4: Detailed support for Proposed Rejection #4, showing that claims 11, 27 and 41 are obvious over Lendenmann under 35 U.S.C. § 103.

U.S. Patent No. 7,188,180*	Chart E-1.4: Claims 11, 27 and 41 are obvious over Lendenmann under 35 U.S.C. § 103
[11.0] The method according to claim 1,	[11.0] <i>The method according to claim 1,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 1.
[11.1] wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.	[11.1] <i>wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.</i> In view of Lendenmann’s disclosure of a secure domain name (portion [1.1]) that is different from a conventional DNS name (portion [2.1b]), a person of ordinary skill in the art would have considered the use of a top level domain name that includes .scom, .snet, .sorg, .sedu, .smil, or .sgov to be a matter of mere design choice. Design choice is “an acceptable rationale for an obviousness rejection when a claimed product merely arranges known elements in a configuration recognized as functionally equivalent to a known configuration.” <i>See, Ex parte Gunasekar</i> , Appeal 2009-008345 in 10/903,590 (BPAI 2011). Since Lendenmann teaches secure domain names that correspond to conventional domain names and since .com, .net, .org, .edu, and .gov are character combinations commonly known to represent top level domain names, arranging the known top level domain name character combinations with the additional known character “s” to abbreviate the descriptive term “security” is an obvious design choice. Thus, the method of claim 1 wherein a secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil, or .sgov would have been obvious in view of Lendenmann.
[27.0] The	[27.0] <i>The computer-readable medium according to claim 17,</i>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-1
Lendenmann

U.S. Patent No. 7,188,180*	Chart E-1.4: Claims 11, 27 and 41 are obvious over Lendenmann under 35 U.S.C. § 103
computer-readable medium according to claim 17,	As analyzed above, Lendenmann teaches all of the limitations of claim 17.
[27.1] wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.	[27.1] <i>wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.</i> See analysis of portion [11.1].
[41.0] The apparatus of claim 33,	[41.0] <i>The apparatus of claim 33,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 33.
[41.1] wherein the secure domain name has a top-level domain name that includes one of scom, .snet, .sorg, .sedu, smil or .sgov.	[41.1] <i>wherein the secure domain name has a top-level domain name that includes one of scom, .snet, .sorg, .sedu, smil or .sgov.</i> See analysis of portion [11.1].

-End-

Exhibit E2

Claim charts applying Kiuchi as a primary reference to the '180 patent.

EXHIBIT E-2
Kiuchi

Contents

Chart E-2.1: Detailed support for Proposed Rejection #5, showing that claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)..... 2

Chart E-2.2: Detailed support for Proposed Rejection #6, showing that claims 3 and 19 are obvious over Kiuchi in view of Masys under 35 U.S.C. § 103. 43

Chart E-2.3: Detailed support for Proposed Rejection #7, showing that claims 7, 23 and 38 are obvious over Kiuchi in view of Martin under 35 U.S.C. § 103. 47

Chart E-2.4: Detailed support for Proposed Rejection #8, showing that claims 11, 27, and 41 are obvious over Kiuchi alone under 35 U.S.C. § 103..... 51

EXHIBIT E-2
Kiuchi

Section 1 – Anticipation

Chart E-2.1: Detailed support for Proposed Rejection #5, showing that claims 1-2, 4-6, 8-10, 12-18, 20-22, 24-26, 28-37, and 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b).

“C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet,” by authors Takahiro Kiuchi and Shigekoto Kaihara published in the Proceedings of Symposium on Network and Distributed System Security 1996 (“Kiuchi”).

Kiuchi is a publication that was publicly available more than one year before the '180 Patent's earliest possible priority date of Oct. 30, 1998 and is prior art under 35 U.S.C. §102(b). A copy of Kiuchi is attached as Exhibit D-2.

As potentially helpful guidance in giving the claims the broadest reasonable interpretation consistent with the specification, the following analysis makes occasional reference to the Patent Owner's prior characterizations of the claims in the first reexamination, and to the claim interpretation from prior litigation involving the '180 patent:

- Reexamination of US 7,188,180, Control No. 95/001,270, Patent Owner Response filed May 24, 2010 [*hereinafter* “Patent Owner Response”]. A copy of the Patent Owner Response is included in Exhibit B-3.
- *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009) [*hereinafter* “E.D. Tex. Order”]. A copy of the E.D. Tex. Order is attached as Exhibit B-4.

The following analysis also refers to the following documents to assist (i) interpreting the claim language under the broadest reasonable interpretation and (ii) understanding the teachings of Kiuchi in accordance with MPEP 2131.01:¹

- “RFC 793”: Information Sciences Institute, “Transmission Control Protocol,” DARPA Internet Program Protocol Specification RFC 793 (Sept. 1981).

RFC 793 is a printed publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b). A copy of RFC 793 is attached as Exhibit D-6.

¹ A second or subsequent reference may be referenced in a rejection under 35 U.S.C. § 102 “when the extra references are cited to: (A) Prove the primary reference contains an ‘enabled disclosure;’ (B) Explain the meaning of a term used in the primary reference; or (C) Show that a characteristic not disclosed in the reference is inherent.” MPEP 2131.01.

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>[1.0] A method for accessing a secure computer network address, comprising steps of:</p>	<p>[1.0] <i>A method for accessing a secure computer network address, comprising steps of:</i></p> <p>Kiuchi teaches accessing a secure computer network address.</p> <p>Specifically, Kiuchi describes “the design and implementation of a closed HTTP (Hypertext Transfer Protocol)-based network (C-HTTP).” (Kiuchi at 64.) C-HTTP “provides <i>secure HTTP communication mechanisms within a closed group of institutions</i> on the Internet, where each member is protected by its own firewall.” (Kiuchi, Abstract at 64, emphasis added.) The institutions “communicate with each other using a <i>secure, encrypted protocol.</i>” (<i>Id.</i>, emphasis added.)</p> <p>Kiuchi further describes that a “client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol.” (Kiuchi at 64.) Further, “Both the request to and response from the C-HTTP name server are encrypted and certified, using asymmetric key encryption and digital signature technology.”(Kiuchi at 65.)</p> <p>Kiuchi describes the various C-HTTP technologies used to secure the client-side and server-side proxies, including encryption and authentication:</p> <p style="padding-left: 40px;">In C-HTTP, five kinds of <i>security technologies</i> are used. They are: 1) asymmetric key <i>encryption</i> for the <i>secure exchange</i> of data <i>encryption</i> keys between two types of proxies and host information between a proxy and C-HTTP name server, 2) symmetric key <i>encryption</i> for the <i>encryption</i> of C-HTTP <i>encrypted</i> headers and HTTP/1.0 requests, 3) electronic signature for the request/response <i>authentication</i>, 4) a one-way hash function for checking data tampering and</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>5) random key generation technology.</p> <p>(Kiuchi at 64, emphasis added.)</p> <p>Kiuchi further describes that the client-side proxy requests access to a secure server-side proxy computer that has a network address, namely an IP address:</p> <p style="padding-left: 40px;">A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. <i>If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy</i> and both request and response Nonce values.</p> <p>(Kiuchi at 65, emphasis added.)</p> <p>It is understood that engaging in secure communication, such as by encrypting exchanges and requiring authentication between a client and a server, to access the IP address of the secure server-side proxy is “accessing a secure computer network address” as claimed.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10.)</p> <p>Thus, Kiuchi teaches a “method for accessing a secure computer network address” as claimed.</p>
<p>[1.1] receiving a secure domain</p>	<p>[1.1] <i>receiving a secure domain name</i></p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
name;	<p>Kiuchi discloses receiving a secure domain name.</p> <p>Specifically, Kiuchi discloses that the client-side proxy receives a “given URL” from a user. The given URL specifies a hostname for a server-side proxy with which the client-side proxy seeks to communicate:</p> <p style="padding-left: 40px;">A client-side proxy asks the C-HTTP name server whether it can communicate with the <i>host specified in a given URL</i>. If the name server confirms that the query is legitimate, it examines whether the <i>requested server-side proxy</i> is registered in the closed network and is permitted to accept the connection from the client-side proxy.</p> <p>(Kiuchi at 65, emphasis added.)</p> <p>Kiuchi describes that the secure server-side proxy registers an IP address, a port number, and “a hostname (<i>which does not have to be the same as its DNS name</i>)” (Kiuchi at 65, emphasis added). The hostname for the secure server-side proxy specified in the given URL is a secure domain name.</p> <p>Access to the secure server-side proxy by the client-side proxy is controlled, in part, by C-HTTP’s own secure name service:</p> <p style="padding-left: 40px;">As C-HTTP includes its own <i>secure name service</i>, which contains a certification mechanism, it is impossible to know the IP address of a server-side proxy even if its C-HTTP hostname (not necessarily the same as its DNS name) is known and visa versa. The <i>C-HTTP name service is efficient because it can do name resolution</i> and host certification simultaneously.</p> <p>(Kiuchi at p. 68, emphasis added.)</p> <p>Kiuchi distinguishes the secure name service of C-HTTP from a conventional DNS, stating that “[i]n a C-HTTP-based network, instead of a DNS, a C-HTTP-based secure, encrypted name and certification service is used.” (Kiuchi at p. 64)</p> <p>Thus, Kiuchi’s disclosure of obtaining, from a user, a hostname specified</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
	<p>in a given URL, which identifies a requested secure server-side proxy, is “receiving a secure domain name.”</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the patent owner asserts that the phrase “secure domain name” refers to a name that “cannot be resolved by a conventional domain name service.” (Patent Owner Response at 6.)</p> <p>Kiuchi distinguishes the C-HTTP name server, which can resolve a host name specified in URL identifying a secure server-side proxy, from a conventional domain name server. For example, Kiuchi describes verifying a client-side proxy’s authorization as part of the name-lookup process:</p> <p style="padding-left: 40px;">A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. <i>If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values. If it is not permitted, it sends a status code which indicates an error.</i> If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.</p> <p>(Kiuchi at 65, emphasis added.)</p> <p>Because a user must be authenticated and authorized in order to resolve a name, the name is a “secure domain name.” For example, a client-side proxy cannot resolve the network address of the name unless it is authorized, and therefore unauthorized users cannot communicate with the corresponding IP address.</p> <p>As shown in Kiuchi Appendix 3, the secure server-side proxy is identified by the secure domain name, i.e. “hostname,” “Coordinating.Center.CSCRG.”</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
	<p>Appendix 3. Examples of C-HTTP communication (a-h)</p> <p>Note that lines with an asterisk are encrypted. Components of C-HTTP-based communication are as follows:</p> <ol style="list-style-type: none">1) Client-side proxy hostname: University of Tokyo.Branch.Hospital IP address: 130.69.111.1112) server-side proxy hostname: Coordinating.Center.CSCRG IP address: 130.69.222.222 port number: 80803) C-HTTP name server: Name.Server.CSCRG IP address: 130.69.222.1114) User agent: IP address: 192.168.123.123 <p>(Kiuchi at p. 73)</p> <p>As evidence that this interpretation is also within the broadest reasonable interpretation of a person of skill in the art, note that the patent owner asserted that the phrase “secure domain name” may alternatively refer to a name of a computer with which no communications are possible without authorization. (Patent Owner Response at 6-7.)</p> <p>In addition, a federal court interpreted the phrase “secure domain name” to refer to a “domain name that corresponds to a secure computer network address.” (E.D. Tex. Opinion at 31.) The court interpreted a secure computer network address to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (<i>Id.</i> at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10)</p> <p>Thus, Kiuchi teaches “receiving a secure domain name” as recited in the claim.</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>[1.2a] sending a query message to a secure domain name service, [1.2b] the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[1.2a] <i>sending a query message to a secure domain name service</i></p> <p>Kiuchi teaches sending a query message to a secure domain name service.</p> <p>Specifically, Kiuchi discloses the secure C-HTTP name service:</p> <p style="padding-left: 40px;">As C-HTTP includes its own <i>secure name service</i>, which contains a certification mechanism, it is impossible to know the IP address of a server-side proxy even if its C-HTTP hostname (not necessarily the same as its DNS name) is known and visa versa. The C-HTTP name service is efficient because it can do name resolution and host certification simultaneously.</p> <p>(Kiuchi at p. 68, emphasis added.)</p> <p>Kiuchi describes that the client-side proxy sends a query message to the secure domain name service, namely the C-HTTP name server, to perform a look up for the requested server-side proxy information:</p> <p style="padding-left: 40px;"><i>A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy.</i></p> <p>(Kiuchi at 65, emphasis added.)</p> <p>Further regarding the security of the C-HTTP name server: “The C-HTTP name server manages its own private and public asymmetric keys and the public keys of all proxies which participate in the closed network.” (Kiuchi at 65.)</p> <p>Kiuchi provides the following example C-HTTP query message from a client-side proxy request to the secure C-HTTP name server requesting the C-HTTP name service to look up the server-side proxy’s computer network address corresponding to the secure hostname:</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>Appendix 3. Examples of C-HTTP communication (a-h)</p> <p>Note that lines with an asterisk are encrypted. Components of C-HTTP-based communication are as follows:</p> <p>1) Client-side proxy hostname: University.of.Tokyo.Branch.Hospital IP address: 130.69.111.111</p> <p>2) server-side proxy hostname: Coordinating.Center.CSCRG IP address: 130.69.222.222 port number: 8080</p> <p>3) C-HTTP name server: Name.Server.CSCRG IP address: 130.69.222.111</p> <p>4) User agent: IP address: 192.168.123.123</p> <p>a. Lookup of server-side proxy information (C-HTTP name service protocol)</p> <pre>C-HTTPNS/0.1<CR><LF> RSA<CR><LF> 74<CR><LF> RSA<CR><LF> 32<CR><LF> MD5<CR><LF> <CR><LF> *SERVER<CR><LF> *130.69.111.111<CR><LF> *192.168.123.123<CR><LF> *Coordinating.Center.CSCRG<CR><LF> *8080<CR><LF> <CR><LF> *827ac79ba214769ea2998249bdb9aa97</pre> <p>(Kiuchi at p. 73)</p> <p>As analyzed above in portion [1.1], Kiuchi’s disclosure of a hostname specified in a given URL, which identifies a requested secure server-side proxy is a secure domain name. Kiuchi teaches that a client-side proxy resolves such a secure domain name into a corresponding secure network address by sending a query to the C-HTTP name server.</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
	<p>For these reasons, the C-HTTP name server is a “secure domain name service,” as recited in the claim.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserts that a “secure domain name service” is a name service that “is different from a conventional domain name service.” (Patent Owner Response at 8.) As analyzed above in portion [1.1], Kiuchi discloses that the C-HTTP name server is a non-conventional domain name service to resolve secure domain names.</p> <p>Thus, Kiuchi teaches “sending a query message to a secure domain name service” as claimed.</p> <hr/> <p>[1.2b] <i>the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name</i></p> <p>Kiuchi teaches that the query message requests, from the secure C-HTTP name service, a secure computer network address corresponding to the secure domain name.</p> <p>As analyzed above in portion [1.1] and [1.2a], Kiuchi teaches that the secure C-HTTP name service provides a secure computer network address in response to a name query:</p> <p style="padding-left: 40px;">A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. <i>If the connection is permitted, the C-HTTP name server sends the IP address</i> and public key of the server-side proxy and both request and response Nonce values. If it is not permitted, it sends a status code which indicates an error. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
	<p>(Kiuchi at 65, emphasis added.)</p> <p>And as analyzed above in portion [1.1], a host name for a secure server-side proxy, as taught by Kiuchi, is a “secure domain name.”</p> <p>Kiuchi further teaches that the IP address returned by the C-HTTP name service is a “secure computer network address.” As disclosed, the IP address of the server-side proxy is kept secure by the certification mechanisms of the C-HTTP name service:</p> <p style="padding-left: 40px;">As C-HTTP includes its own secure name service, which contains a certification mechanism, <i>it is impossible to know the IP address of a server-side proxy even if its C-HTTP hostname (not necessarily the same as its DNS name) is known and visa versa.</i> The C-HTTP name service is efficient because it can do name resolution and host certification simultaneously.</p> <p>(Kiuchi at p. 68, emphasis added.)</p> <p>Since only authorized client-side proxies are permitted to obtain a network address from the secure C-HTTP name service, it is understood that unauthorized users and clients cannot communicate with or access the network address. Thus, Kiuchi teaches that only authorized clients and users can communicate with or access the network address associated with a secure domain name.</p> <p>Accordingly, the network address of a secure server-side proxy, as described in Kiuchi, is a “secure computer network address,” under at least the broadest reasonable interpretation.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserted that a secure computer network address is an address that requires authorization for access or communication. See, for example, Patent Owner Response at 6 (stating that “the computers ... themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them.”).</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>In addition, a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (Id. at 10.)</p> <p>Thus, Kiuchi teaches “sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.3] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name;</p>	<p>[1.3] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name</i></p> <p>Kiuchi discloses receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.</p> <p>Specifically, Kiuchi discloses that the secure C-HTTP name service returns to the client-side proxy a response that includes the secure computer network address for the secure domain name:</p> <p style="padding-left: 40px;">A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. <i>If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy</i> and both request and response Nonce values. If it is not permitted, it sends a status code which indicates an error. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.</p> <p>(Kiuchi at 65, emphasis added.)</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>As shown further in example 2.2 of the Kiuchi Appendix 2, the C-HTTP name service response includes the secure server-side IP address that corresponds to the requested hostname:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>2.2 C-HTTP name service response</p> </div> <pre> ENCRYPTION-ALGORITHM <CR><LF> ENCRYPTED-PART-LENGTH <CR><LF> SIGNATURE-ALGORITHM <CR><LF> SIGNATURE-LENGTH <CR><LF> MESSAGE-DIGEST-ALGORITHM <CR><LF> <CR><LF> *C-HTTP-NAME-SERVICE-STATUS <CR><LF> *CLIENT-SIDE-PROXY-IP <CR><LF> *USER-AGENT-IP <CR><LF> *SERVER-SIDE-PROXY-IP <CR><LF> *SERVER-SIDE-PROXY-PORT <CR><LF> *SERVER-SIDE-PROXY-PUBLIC-KEY <CR><LF> *REQUEST-NONCE <CR><LF> *RESPONSE-NONCE <CR><LF> <CR><LF> *DIGITAL-SIGNATURE </pre> <p>(Kiuchi at p. 72-73.)</p> <p>As previously analyzed in portion [1.2b], a secure server-side proxy IP address, as described in Kiuchi, is a “secure computer network address,” under at least the broadest reasonable interpretation. And as previously analyzed in portion [1.1], a hostname as described in Kiuchi is a “secure domain name,” under at least the broadest reasonable interpretation.</p> <p>Thus, Kiuchi teaches “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.4a] and sending an access request message to the secure computer network address [1.4b] using a virtual private network communication</p>	<p>[1.4a] and sending an access request message to the secure computer network address</p> <p>Kiuchi teaches sending an access request message to the secure computer network address. Specifically, Kiuchi teaches that a client-side proxy sends a request to access the secure server-side proxy:</p> <p style="padding-left: 40px;">When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>link.</p>	<p><i>client-side proxy sends a request for connection to the server-side proxy</i>, which is encrypted using the server-side proxy's public key and contains the client-side proxy's IP address, hostname, request Nonce value and symmetric data exchange key for request encryption.</p> <p>(Kiuchi at p. 65, emphasis added.)</p> <p>The request for connection is an "access request message" as recited in the claim.</p> <p>As shown Kiuchi's Appendix 3, the request to access the secure server-side proxy includes the server-side proxy's IP address:</p> <div data-bbox="500 947 995 989" style="border: 1px solid black; padding: 2px;"> <p>c. Request for connection to the server-side proxy</p> </div> <pre>CONNECT C-HTTP/0.7
 Encryption-Algorithm: RSA
 Encrypted-Header-Length: 298
 Signature-Algorithm: RSA
 Signature-Length: 32
 Message-Digest-Algorithm: MD5
 *Client-Side-Proxy-IP: 130.69.109.111.111
 *Client-Side-Proxy-Name: University of Tokyo Branch Hospital
 *User-Agent-IP: 192.168.123.123
 *Server-Side-Proxy-IP: 130.69.222.222
 *Server-Side-Proxy-Name: Coordinating Center CSCRG
 *Server-Side-Proxy-Port: 8080
 *Data-Exchange-Key-Request: #8Jk=d n,&1i's
 *Request-Nonce: 8abd855f
 *4d3b8ea8060040a38d1a3aab34ce2cb8</pre> <p>(Kiuchi at p. 74)</p> <p>Thus, Kiuchi teaches "sending an access request message to the secure computer network address" as recited in the claim.</p> <hr/> <p>[1.4b] using a virtual private network communication link.</p> <p>Kiuchi teaches that the communication link established between the</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
	<p>client-side proxy and server-side proxy may be a virtual private network.</p> <p>Specifically, Kiuchi discloses: “Using C-HTTP, a closed HTTP-based <i>virtual network</i> can be created <i>for closed groups</i>; for example, the headquarters and branches of a given corporation.” (Kiuchi at p. 69, emphasis added)</p> <p>Kiuchi distinguishes C-HTTP communication from ordinary HTTP: “In C-HTTP, as different from ordinary HTTP, a session (<i>virtual C-HTTP connection</i>) is established between a client-side proxy and a server-side proxy and, thus, is not stateless. (Kiuchi at p. 65, emphasis added.)</p> <p>Further, Kiuchi teaches that the secure communication between the client-side proxy and the server-side proxy is encrypted:</p> <p style="padding-left: 40px;">When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client-side proxy sends <i>a request</i> for connection to the server-side proxy, <i>which is encrypted using the server-side proxy’s public key</i> and contains the client-side proxy’s IP address, hostname, request Nonce value and <i>symmetric data exchange key for request encryption</i>.</p> <p>(Kiuchi at p. 65, emphasis added.)</p> <p>Regarding communication encryption, Kiuchi further discloses that “[a] client-side proxy and server-side proxy communicate with each other using a secure, <i>encrypted</i> protocol (C-HTTP).” (Kiuchi at p. 64.) The secure communication link is facilitated by “asymmetric key encryption for the secure exchange of data <i>encryption keys</i> between two types of proxies” (Kiuchi at p. 64)</p> <p>Kiuchi further discloses that request messages must be authenticated:</p> <p style="padding-left: 40px;">In C-HTTP, five kinds of security technologies are used. They are: 1) asymmetric key encryption for the secure exchange of data encryption keys between two types of proxies and host information between a proxy and C-HTTP name server, 2) symmetric key encryption for the encryption of C-HTTP encrypted headers and HTTP/1.0 requests, 3)</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>electronic signature for the request/response <i>authentication</i>, 4) a one-way has function for checking data tampering and 5) random key generation technology.</p> <p>(Kiuchi at 64, emphasis added.)</p> <p>Kiuchi further discloses that the secure C-HTTP virtual network is built on the otherwise insecure Internet: “In this paper, we discuss the design and implementation of a <i>closed HTTP (Hypertext Transfer Protocol)-based network (C-HTTP) which can be built on the Internet</i>. (Kiuchi at p. 64) Additionally, the title of the Kiuchi article is “C-HTTP – The Development of a <i>Secure, Closed HTTP-based Network on the Internet</i>” (Kiuchi at p. 64)</p> <p>In summary, Kiuchi teaches that requests and responses between the client-side and server-side proxies include authentication of client and server identities and encryption. Thus, Kiuchi teaches that communications via a request procedure may be secure and private even when conducted over an insecure communication path, such as the Internet.</p> <p>By creating a “virtual network” for closed groups and by providing authenticated and encrypted communications between client-side and server-side proxies over the Internet, Kiuchi teaches sending an access request message “using a virtual private network communication link” as recited in the claim.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (E.D. Tex. Opinion at 10.)</p> <p>Thus, Kiuchi teaches sending an access request message “using a virtual private network communication link” as recited in the claim.</p>
<p>[2.0] The method according to claim 1, wherein the step</p>	<p>[2.0] <i>The method according to claim 1, wherein the step of receiving the secure domain name includes steps of:</i></p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>of receiving the secure domain name includes steps of:</p>	<p>As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>
<p>[2.1a] receiving a command to establish the virtual private network communication link [2.1b] with a secure computer network address corresponding to a predetermined non-secure domain name; and</p>	<p>[2.1a] <i>receiving a command to establish the virtual private network communication link</i></p> <p>As previously analyzed in portion [1.1], Kiuchi teaches receiving a command to establish a virtual private network communication link. For example, a client-side proxy receives a user command that includes a secure domain name:</p> <p style="padding-left: 40px;">When one of these resource names with a connection ID, for example, <code>http://server.in.current.connection/sample.html=@=6zdDfl dfcZLj8V!i</code> in Figure (b), is selected and <i>requested by an end-user</i>, the client-side proxy takes off the connection ID and forwards the stripped, the original resource name to the server in its request as described in Figure (c).</p> <p>(Kiuchi at p. 65, emphasis added.)</p> <p>This initial user command results in the establishment of the virtual private network communication link. As previously analyzed in portion [1.4a] & [1.4b], Kiuchi teaches a client-side proxy connection request procedure that may include checks on authentication and encryption. The connection request is sent using a “virtual private network communication link” as recited. Thus, the initial user command results in the establishment of the virtual private network communication link.</p>
	<p>[2.1b] <i>with a secure computer network address corresponding to a predetermined non-secure domain name</i></p> <p>Kiuchi discloses a secure computer network address corresponding to a predetermined non-secure domain name.</p> <p>As described above in portion [1.2b], Kiuchi discloses a secure computer network address corresponding to a secure domain name. Kiuchi also</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>describes that the secure hostname, and therefore the corresponding secure computer network address, may correspond to a conventional “DNS name,” i.e., a non-secure domain name:</p> <p style="padding-left: 40px;">When a given institution wants to participate in a closed network, it must . . . 2) register an IP address (for a server-side proxy, a port number should also be registered) and <i>hostname (which does not have to be the same as its DNS name)</i> for a firewall gateway. . .</p> <p>(Kiuchi at p. 65, emphasis added.)</p> <p>The corresponding secure and non-secure domain names are further described:</p> <p style="padding-left: 40px;">As C-HTTP includes its own secure name service, which contains a certification mechanism, it is impossible to know the IP address of a server-side proxy even if its <i>C-HTTP hostname (not necessarily the same as its DNS name)</i> is known and visa versa. The C-HTTP name service is efficient because it can do name resolution and host certification simultaneously.</p> <p>(Kiuchi at p. 68, emphasis added.)</p> <p>Thus, Kiuchi teaches that the secure hostname may also have a conventional DNS name, which is a “predetermined non-secure domain name” as recited in the claim. Kiuchi, therefore, teaches a correspondence between the secure computer network address and both secure and non-secure domain names.</p>
<p>[2.2] automatically generating a secure domain name corresponding to the non-secure domain name.</p>	<p>[2.2] <i>automatically generating a secure domain name corresponding to the non-secure domain name.</i></p> <p>Kiuchi discloses automatically generating a secure domain name corresponding to a non-secure domain name.</p> <p>As explained in portion [1.1] above, the server-side proxy has a “hostname” which is a secure domain name as claimed. The hostname is specified in, and therefore may be automatically generated from, a “given</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>URL”: “A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL.”</p> <p>The same hostname may be generated from the URL without any user involvement, in other words, “automatically.” In fact, end users “do not even have to be conscious of using C-HTTP based communications.” (Kiuchi at p. 68)</p> <p>As described in portion [2.1b], the secure hostname corresponds to the non-secure DNS name.</p> <p>Therefore, Kiuchi discloses generating a secure domain name that corresponds to a non-secure domain name.</p>
<p>[4.0] The method according to claim 1,</p>	<p>[4.0] <i>The method according to claim 1</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>
<p>[4.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[4.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>Kiuchi discloses that the response message received from the secure domain name service contains provisioning information for the virtual private network.</p> <p>For example, Kiuchi teaches that the response from the C-HTTP name server includes provisioning information to make a virtual private network link available, including encryption keys and Nonce values used for authentication:</p> <p>A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. <i>If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values.</i> If it is not permitted, it sends a status code which indicates an error. If a client-side proxy receives an error status, then it performs DNS lookup,</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>behaving like an ordinary HTTP/1.0 proxy.</p> <p>(Kiuchi at 65, emphasis added.)</p> <p>As shown further in example 2.2 of the Kiuchi Appendix 2, the C-HTTP name service response includes the secure server-side proxy public key and request/response Nonce values.</p> <p>2.2 C-HTTP name service response</p> <pre> ENCRYPTION-ALGORITHM<CR><LF> ENCRYPTED-PART-LENGTH<CR><LF> SIGNATURE-ALGORITHM<CR><LF> SIGNATURE-LENGTH<CR><LF> MESSAGE-DIGEST-ALGORITHM<CR><LF> <CR><LF> *C-HTTP-NAME-SERVICE-STATUS<CR><LF> *CLIENT-SIDE-PROXY-IP<CR><LF> *USER-AGENT-IP<CR><LF> *SERVER-SIDE-PROXY-IP<CR><LF> *SERVER-SIDE-PROXY-PORT<CR><LF> *SERVER-SIDE-PROXY-PUBLIC-KEY<CR><LF> *REQUEST-NONCE<CR><LF> *RESPONSE-NONCE<CR><LF> <CR><LF> *DIGITAL-SIGNATURE </pre> <p>(Kiuchi at p. 72-73.)</p> <p>The public key and the Nonce values are “provisioning information.”</p> <p>Thus, Kiuchi teaches that “the response message contains provisioning information for the virtual private network” as recited in the claim.</p>
<p>[5.0] The method according to claim 4,</p>	<p>[5.0] <i>The method according to claim 4,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 4.</p>
<p>[5.1] wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer</p>	<p>[5.1] <i>wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address,</i></p> <p>Kiuchi teaches that the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address.</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>network address,</p>	<p>Specifically, Kiuchi teaches that the virtual private network (<i>See</i>, portion [1.4b]) is based on inserting randomly generated bytes into requests and responses:</p> <p style="padding-left: 40px;">C-HTTP name service protocol is different from other parts of the C-HTTP in the following points:</p> <p style="padding-left: 40px;">...</p> <p style="padding-left: 40px;">3) <i>Random bytes are inserted every fourth byte of the request and response</i> before encryption in order to avoid the same encrypted requests or responses being repeated. This is useful to make it impossible to predict the server-side proxy which will be connected after the name request.</p> <p>(Kiuchi Appendix 2. at p. 72, emphasis added.)</p> <p>Thus, Kiuchi teaches that the virtual private network is based on inserting randomly generated bytes into each request sent to the secure server-side proxy associated with the secure computer network address.</p>
<p>[5.2] the one or more data values varying according to a pseudo-random sequence.</p>	<p>[5.2] <i>the one or more data values varying according to a pseudo-random sequence.</i></p> <p>Kiuchi teaches that the one or more data values vary according to a pseudo-random sequence.</p> <p>As described in portion [5.1], the inserted data values vary randomly. Because these “random” bytes are generated by the C-HTTP name service protocol, which relies on a methodical computer algorithm, they are understood to be a “pseudo-random” sequence, as recited in the claim.</p>
<p>[6.0] The method according to claim 4,</p>	<p>[6.0] <i>The method according to claim 4,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 4.</p>
<p>[6.1] wherein the virtual private network is based on inserting into at least one data</p>	<p>[6.1] <i>wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</i></p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
<p>packet at least one data value representing a predetermined level of service associated with the virtual private network.</p>	<p>Kiuchi discloses that the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</p> <p>Kiuchi teaches that communication in the virtual private network (<i>See</i>, portion [1.4b]) occurs over a TCP/IP session. Specifically, Kiuchi teaches that “C-HTTP itself is stateful, but the TCP connection is closed after each transaction (request and response pair) in order to reduce the possibility of it being intercepted by attackers.” (Kiuchi at p. 67)</p> <p>The transmission control protocol (TCP) is defined in RFC 793, which describes the use of a type of service field which indicates a precedence (i.e., a level) and security of service:</p> <p style="padding-left: 40px;">The TCP makes use of the internet protocol <i>type of service field</i> and security option to provide precedence and security on a per connection basis to TCP users.</p> <p>(RFC 793 at p. 12, emphasis added.)</p> <p>It is understood that Kiuchi’s request and response transactions, which run over TCP, use “a data value representing a predetermined level of service” as recited in the claim.</p>
<p>[8.0] The method according to claim 4,</p>	<p>[8.0] <i>The method according to claim 4</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 4.</p>
<p>[8.1] wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</p>	<p>[8.1] <i>wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</i></p> <p>Kiuchi teaches that the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</p> <p>Specifically, Kiuchi teaches that the virtual private network (<i>See</i>, portion [1.4b]) is established and maintained by comparing Nonce values found in requests to the secure server-side proxy to the valid Nonce values</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>generated by the C-HTTP name service. The Nonce are valid for only a limited window of time:</p> <p>If access is permitted, <i>the C-HTTP name server sends the IP address and public key of the client-side proxy and both request and response Nonce values</i>, which are the same as those sent to the client-side proxy. <i>The C-HTTP name server keeps both of the Nonce values for thirty seconds.</i> If not, it sends a status code which indicates an error and the server-side proxy refuses the connection from the client-side proxy. . . . When the server-side proxy obtains the client-side proxy’s IP address, hostname, and public key, it authenticates the client-side proxy, <i>checks the integrity of the request and the request Nonce value . . .</i></p> <p>(Kiuchi at p. 66, emphasis added.)</p> <p>In the Examples of C-HTTP communication found in Appendix 3, it can be seen that the “Request-Nonce” value is incremented, moving from “8abd853f” in Example c., to “8abd8540” in Example g., to “8abd8541” in Example i.</p> <p>c. Request for connection to the server-side proxy</p> <pre>CONNECT C-HTTP/0.7
 Encryption-Algorithm: RSA
 Encrypted-Header-Length: 298
 Signature-Algorithm: RSA
 Signature-Length: 32
 Message-Digest-Algorithm: MD5

 *Client-Side-Proxy-IP: 130.69.109.111.111
 *Client-Side-Proxy-Name: University of Tokyo Branch Hospital
 *User-Agent-IP: 192.168.123.123
 *Server-Side-Proxy-IP: 130.69.222.222
 *Server-Side-Proxy-Name: Coordinating Center, CSCRG
 *Server-Side-Proxy-Port: 8080
 *Data-Exchange-Key-Request: #8R=8 q.&H's
 *Request-Nonce: 8abd853f

 *4d3b8ea8060046a38d1a3aab34ce2cb8</pre>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>g. Sending C-HTTP requests to the server-side proxy</p> <p>REQUEST C-HTTP/0.7<CR><LF> Encryption-Algorithm:DES-CBC, B0s9cb01a93a8df <CR><LF></p> <p>Encrypted-Header-Length: 349<CR><LF> Encrypted-HTTP-1.0-Length: 31<CR><LF> Signature-Algorithm: RSA<CR><LF> Signature-Length: 32<CR><LF> Message-Digest-Algorithm: MD5<CR><LF> <CR><LF></p> <p>*Server-Side-Proxy-IP: 130.69.222.222<CR><LF> *Server-Side-Proxy-Name: Coordinating.Center.CSCRG<CR><LF> *Server-Side-Proxy-Port: 8080<CR><LF> *Client-Side-Proxy-IP: 130.69.111.111<CR><LF> *Client-Side-Proxy-Name: University.of.Tokyo.Branch.Hospital<CR><LF> *User-Agent-IP: 192.168.123.123<CR><LF> *Connection-ID: 6zd0dfdfc7118Vll<CR><LF> *Request-Nonce: 8abd8540<CR><LF></p> <p>*<HTTP/1.0 Request> <CR><LF> *2ec7d37d0ac2c15ddc455c45913affb6</p> <p>i. Request for closing the connection</p> <p>CLOSE<SP> C-HTTP/0.7<CR><LF> Encryption-Algorithm: DES-CBC, acd42bef76gf3b98<CR><LF> Encrypted-Header-Length: 349<CR><LF></p> <p>Signature-Algorithm: RSA<CR><LF> Signature-Length: 32<CR><LF> Message-Digest-Algorithm: MD5<CR><LF> <CR><LF></p> <p>*Client-Side-Proxy-IP: 130.69.111.111<CR><LF> *Client-Side-Proxy-Name: University.of.Tokyo.Branch.Hospital<CR><LF> *User-Agent-IP: 192.168.123.123<CR><LF> *Server-Side-Proxy-IP: 130.69.222.222<CR><LF> *Server-Side-Proxy-Name: Coordinating.Center.CSCRG<CR><LF> *Server-Side-Proxy-Port: 8080<CR><LF> *Connection-ID: 6zd0dfdfc7118Vll<CR><LF> *Request-Nonce: 8abd8541<CR><LF></p> <p><CR><LF> *c37d7b17f13efce24e7a9ac6858d0293</p> <p>Thus, Kiuchi teaches that the virtual private network is based on comparing a Nonce value in each request sent to a secure server-side</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>proxy to a moving window of valid Nonce values created by the C-HTTP name service.</p>
<p>[9.0] The method according to claim 4,</p>	<p>[9.0] <i>The method according to claim 4</i> As analyzed above, Kiuchi teaches all of the limitations of claim 4.</p>
<p>[9.1a] wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address [9.1b] to a table of valid discriminator fields.</p>	<p>[9.1a] <i>wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address</i> Kiuchi teaches that the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address. Specifically, Kiuchi teaches that the virtual private network (<i>See</i>, portion 1.4b) is based on a comparison of a connection ID field in the header of a request to the secure server-side proxy associated with the secure computer network address. The server-side proxy generates the connection ID: When <i>the server-side proxy</i> obtains the client-side proxy's IP address, hostname and public key, it authenticates the client-side proxy, checks the integrity of the request and the request Nonce value and <i>generates</i> both <i>a connection ID</i> derived from the server-side proxy's name, date and random numbers (32 bits) using MD5, and also a second symmetric data exchange key for response encryption, which are sent to the client-side proxy. (Kiuchi at p. 66, emphasis added) The connection ID is included in the header of C-HTTP requests sent from the client-side proxy to the server-side proxy over the virtual private network communication link: g. Sending C-HTTP requests to the server-side proxy REQUEST C-HTTP/0.7 <ip> <port> Encryption-Algorithm:DES-CBC, f30a9cb01a93a8df <CR><LF></p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<pre> Encrypted-Header-Length: 349<CR><LF> Encrypted-HTTP/1.0-Length: 31<CR><LF> Signature-Algorithm: RSA<CR><LF> Signature-Length: 32<CR><LF> Message-Digest-Algorithm: MD5<CR><LF> <CR><LF> *Server-Side-Proxy-IP: 130.69.222.222<CR><LF> *Server-Side-Proxy-Name: Coordinating Center CSCRG<CR><LF> *Server-Side-Proxy-Port: 8080<CR><LF> *Client-Side-Proxy-IP: 130.69.111.111<CR><LF> *Client-Side-Proxy-Name: University of Tokyo Branch Hospital<CR><LF> *User-Agent-IP: 193.168.123.123<CR><LF> *Connection-ID: 6zedDfdfc2Lj8VH<CR><LF> *Request-Nonce: 8abd8540<CR><LF> *-<HTTP/1.0 Request> <CR><LF> *2ec7d37d0ac2c15dde455c45913affe6 </pre> <p>Thus, Kiuchi teaches that the virtual private network is based on a comparison of a discriminator field, namely the connection ID, in a header of each request sent to the secure server-side proxy associated with the secure computer network address.</p> <hr/> <p>[9.1b] <i>to a table of valid discriminator fields</i></p> <p>Kiuchi teaches that the discriminator field is compared to a table of valid discriminator fields.</p> <p>Specifically, Kiuchi discloses a “current connection table” or “connection list” to which the connection ID is compared: “When the connection ID is not found in the <i>current connection table</i> in the client-side-proxy, the current connection is disconnected.” (Kiuchi at p. 65, emphasis added) Further, “if the server-side proxy detects that a given connection times out, it deletes the connection ID from the <i>connection list</i>, informing the client-side proxy that the connection is closed when an error status is returned in response to the request.” (Kiuchi at p. 67, emphasis added)</p> <p>Thus, Kiuchi teaches the table as claimed.</p>
<p>[10.0] The method according to claim 1,</p>	<p>[10.0] <i>The method according to claim 1,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>[10.1] wherein the virtual private network includes the Internet.</p>	<p>[10.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>Kiuchi discloses that the virtual private network includes the Internet. As described in portion [1.4b], Kiuchi discloses the use of a virtual private network communication link using the C-HTTP communication protocol.</p> <p>Specifically, Kiuchi discloses that the secure C-HTTP virtual network is built on the otherwise insecure Internet: “In this paper, we discuss the design and implementation of a <i>closed HTTP (Hypertext Transfer Protocol)-based network (C-HTTP) which can be built on the Internet.</i> (Kiuchi at p. 64) Additionally, the title of the Kiuchi article is “C-HTTP – The Development of <i>a Secure, Closed HTTP-based Network on the Internet</i>” (Kiuchi at p. 64)</p> <p>Kiuchi further teaches:</p> <p style="padding-left: 40px;">We have designed “C-HTTP” which provides secure HTTP communication mechanisms within a closed group of institutions on the Internet.</p> <p>(Kiuchi Abstract at p. 64, emphasis added.)</p> <p>Kiuchi further explains how C-HTTP contributes to the development of the Internet:</p> <p style="padding-left: 40px;">Although C-HTTP is primarily developed for use in the medical field, it can be used in other areas. Using C-HTTP, a closed HTTP-based virtual network can be constructed for closed groups; for example, the headquarters and branches of a given corporation. This kind of usage may not fit with the spirit of the Internet, but if resources which might otherwise be invested in private circuits are channeled into the Internet, it will contribute to its further development.</p> <p>(Kiuchi at p. 69)</p> <p>Thus, Kiuchi teaches the method of claim 1 wherein the virtual private network includes the Internet.</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>[12.0] The method according to claim 1,</p>	<p>[12.0] <i>The method according to claim 1,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>
<p>[12.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[12.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i></p> <p>As analyzed above at portion [1.4a], Kiuchi teaches the access request message of claim 1. As analyzed above at portion [1.0], Kiuchi also teaches a “secure computer network address,” namely the secure server-side proxy’s IP address. Kiuchi further teaches that the access request message contains a request for the information stored at the server-side proxy that is needed to establish a connection between the client-side proxy and the server-side proxy. The requested connection information, including a connection ID and a second symmetric data exchange key, are provided by the secure server-side proxy:</p> <p style="padding-left: 40px;">When the server-side proxy obtains the client-side proxy’s IP address, hostname and public key, it authenticates the client-side proxy, checks the integrity of the request and the request Nonce value and <i>generates both a connection ID</i> derived from the server-side proxy’s name, date and random numbers (32 bits) using MD5, <i>and also a second symmetric data exchange key</i> for response encryption, which are sent to the client-side proxy.</p> <p>(Kiuchi at p. 66, emphasis added.)</p> <p>Kiuchi further describes:</p> <p style="padding-left: 40px;">From the view of the user agent or client-side proxy, <i>all resources appear to be located in a server-side proxy</i> on the firewall. In reality, however, the server-side proxy forwards requests to the origin server. It is possible to map any of the virtual directories on the server-side proxy to any of the directories in one or more origin servers inside the firewall.</p> <p>(Kiuchi at p. 66, emphasis added.)</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>Thus, Kiuchi teaches “the access request message contains a request for information stored at the secure computer network address.”</p>
<p>[13.0] The method of claim 1,</p>	<p>[13.0] <i>The method of claim 1,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>
<p>[13.1] wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</p>	<p>[13.1] <i>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</i> As analyzed above at portion [1.1], Kiuchi teaches receiving the secure domain name. Kiuchi further teaches that the secure domain name is received at a client computer from a user. The client-side proxy taught by Kiuchi is the client computer and acts as a proxy for a user agent: <i>A client-side proxy</i> behaves as an HTTP/1.0 compatible proxy, and it should be specified as <i>a proxy server for external</i> (outside the firewall) <i>access in each user agent</i> within the firewall. (Kiuchi at p. 65, emphasis added.) Requests from the user, for connection to other resources, are processed through the client-side proxy: When one of these resource names with a connection ID, for example, http://server.in.current.connection/sample.html=@=6zdDfl dfcZLj8V!i in Figure (b), is selected and <i>requested by an end-user</i>, the client-side proxy takes off the connection ID and forwards the stripped, the original resource name to the server in its request as described in Figure (c). (Kiuchi at p. 65) The client-side proxy receives the connection requests from the user and reformats the request for communication with the C-HTTP name server. For example, when the user gives the client-side proxy a resource URL, the “client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in [the] given URL.” (Kiuchi at p.</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>65)</p> <p>Thus, Kiuchi teaches “wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user.”</p>
<p>[13.2] wherein sending the query message comprises sending the query message at the client computer;</p>	<p>[13.2] <i>wherein sending the query message comprises sending the query message at the client computer;</i></p> <p>As analyzed above at portion [1.2a], Kiuchi teaches that a query message is sent at the client-side proxy to the secure domain name service, namely the C-HTTP name server. The client-side proxy is the client computer as claimed.</p> <p>Thus, Kiuchi teaches “sending the query message comprises sending the query message at the client computer.”</p>
<p>[13.3] wherein receiving the response message comprises receiving the response message at the client computer,</p>	<p>[13.3] <i>wherein receiving the response message comprises receiving the response message at the client computer,</i></p> <p>As analyzed above at portion [1.3], Kiuchi teaches that the secure C-HTTP name service returns to the client-side proxy a response that includes the secure computer network address for the secure domain name. The client-side proxy is the client computer as claimed.</p> <p>Thus, Kiuchi teaches “receiving the response message comprising receiving the response message at the client computer.”</p>
<p>[13.4] wherein sending the access request message comprises sending the access request message at the client computer.</p>	<p>[13.4] <i>wherein sending the access request message comprises sending the access request message at the client computer.</i></p> <p>As analyzed above at portion [1.4a], Kiuchi teaches that an access request message is sent at the client-side proxy to the secure server-side proxy. The client-side proxy is the client computer as claimed.</p> <p>Thus, Kiuchi teaches “sending the access request message comprises sending the access request message at the client computer.”</p>
<p>[14.0] The method of claim 1,</p>	<p>[14.0] <i>The method of claim 1,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
[14.1] performed by a software module.	<p>[14.1] <i>performed by a software module.</i></p> <p>Kiuchi teaches that each of the method steps recited in claim 1 is performed by a C-HTTP software module. Specifically, Kiuchi discloses that, “C-HTTP proxy <i>software</i>” is used by the proxies in the C-HTTP network. (Kiuchi at p. 67, emphasis added.) As disclosed for claim 13, the client-side proxy performs the method steps of claim 1. Therefore, the client-side proxy may perform the method steps of claim 1 by using the C-HTTP proxy software, which is a software module as claimed.</p>
[15.0] The method of claim 1,	<p>[15.0] <i>The method of claim 1,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 1.</p>
[15.1] performed by a client computer.	<p>[15.1] <i>performed by a client computer.</i></p> <p>See analysis of claim 13.</p>
[16.0] The method of claim 2,	<p>[16.0] <i>The method of claim 2</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 2.</p>
[16.1] wherein receiving the command comprises receiving the command at a client computer from a user.	<p>[16.1] <i>wherein receiving the command comprises receiving the command at a client computer from a user.</i></p> <p>See analysis of claim portions [2.1] and [13.1].</p>
[17.0] A computer-readable storage medium, comprising:	<p>[17.0] <i>A computer-readable storage medium, comprising:</i></p> <p>Kiuchi discloses storing or installing keys and software on a firewall:</p> <p style="padding-left: 40px;">In C-HTTP, keys are <i>stored only on the firewall</i> of a given institution. C-HTTP proxy software is provided as source code, and the keys are designed not to be stored in a separate “key file.”</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
	<p>(Kiuchi at 67.)</p> <p>A C-HTTP based network is made available simply by <i>installing proxies on the firewall</i> and registering their information with the C-HTTP name server.</p> <p>(Kiuchi at 68.)</p> <p>It is understood that a firewall is a computer. Thus, Kiuchi teaches a “computer-readable storage medium” as recited in the claim</p>
<p>[17.1] a storage area; and</p>	<p>[17.1] <i>a storage area; and</i></p> <p>See analysis of portion [17.0]. The computer-readable <i>storage medium</i> includes a “storage area.” For example, Kiuchi discloses storing keys and proxy software on a firewall. Thus, it is understood that the firewall includes a “storage area,” as recited in the claim.</p>
<p>[17.2] computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>[17.2] <i>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</i></p> <p>See analysis of portion [1.0]. It is understood that the proxy software system as taught by Kiuchi includes “computer-readable instructions” as recited in the claim.</p>
<p>[17.3] receiving a secure domain name;</p>	<p>[17.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[17.4] sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network</p>	<p>[17.4] <i>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>address corresponding to the secure domain name;</p>	
<p>[17.5] receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>[17.5] <i>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>
<p>[17.6] sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>[17.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
<p>[18.0] The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:</p>	<p>[18.0] <i>The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 17.</p>
<p>[18.1] receiving a command to establish the virtual private network communication link with a secure computer network address</p>	<p>[18.1] <i>receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and</i></p> <p>See analysis of portions [2.1a]–[2.1b].</p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
corresponding to a predetermined non-secure domain name; and	
[18.2] automatically generating a secure domain name corresponding to the non-secure domain name.	[18.2] <i>automatically generating a secure domain name corresponding to the non-secure domain name.</i> See analysis of portion [2.2].
[20.0] The computer-readable medium according to claim 17,	[20.0] <i>The computer-readable medium according to claim 17,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 17.
[20.1] wherein the response message contains provisioning information for the virtual private network.	[20.1] <i>wherein the response message contains provisioning information for the virtual private network.</i> See analysis of portion [4.1].
[21.0] The computer-readable medium according to claim 20,	[21.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 20.
[21.1] wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random	[21.1] <i>wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random</i> See analysis of portions [5.1]–[5.2].

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
sequence.	
[22.0] The computer-readable medium according to claim 20,	[22.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 20.
[22.1] wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.	[22.1] <i>wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</i> See analysis of portion [6.1].
[24.0] The computer-readable medium according to claim 20,	[24.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 20.
[24.1] wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.	[24.1] <i>wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</i> See analysis of portion [8.1].
[25.0] The computer-readable medium according to claim 20,	[25.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 20.
[25.1] wherein the virtual private	[25.1] <i>wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure</i>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.</p>	<p><i>computer network address to a table of valid discriminator fields.</i></p> <p>See analysis of portions [9.1a]–[9.1b].</p>
<p>[26.0] The computer-readable medium according to claim 17,</p>	<p>[26.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 17.</p>
<p>[26.1] wherein the virtual private network includes the Internet.</p>	<p>[26.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>See analysis of portion [10.1].</p>
<p>[28.0] The computer readable medium of claim 17,</p>	<p>[28.0] <i>The computer readable medium of claim 17,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 17.</p>
<p>[28.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[28.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i></p> <p>See analysis of portion [12.1].</p>
<p>[29.0] The computer-readable medium according to claim 17,</p>	<p>[29.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 17.</p>
<p>[29.1] wherein receiving the secure domain name</p>	<p>[29.1] <i>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</i></p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
comprises receiving the secure domain name at a client computer from a user;	See analysis of portion [13.1].
[29.2] wherein sending the query message comprises sending the query message at the client computer;	[29.2] <i>wherein sending the query message comprises sending the query message at the client computer;</i> See analysis of portion [13.2].
[29.3] wherein receiving the response message comprises receiving the response message at the client computer,	[29.3] <i>wherein receiving the response message comprises receiving the response message at the client computer,</i> See analysis of portion [13.3].
[29.4] wherein sending the access request message comprises sending the access request message at the client computer.	[29.4] <i>wherein sending the access request message comprises sending the access request message at the client computer.</i> See analysis of portion [13.4].
[30.0] The computer-readable medium according to claim 17,	[30.0] <i>The computer-readable medium according to claim 17,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 20.
[30.1] wherein the method is performed by a software module.	[30.1] <i>wherein the method is performed by a software module.</i> See analysis of portion [14.1].
[31.0] The computer-readable	[31.0] <i>The computer-readable medium according to claim 17,</i>

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>medium according to claim 17,</p>	<p>As analyzed above, Kiuchi teaches all of the limitations of claim 17.</p>
<p>[31.1] wherein the method is performed by a client computer.</p>	<p>[31.1] <i>wherein the method is performed by a client computer.</i></p> <p>See analysis of portion [15.1].</p>
<p>[32.0] The computer-readable medium according to claim 18,</p>	<p>[32.0] <i>The computer-readable medium according to claim 18,</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 18.</p>
<p>[32.1] wherein receiving the command comprises receiving the command at a client computer from a user.</p>	<p>[32.1] <i>wherein receiving the command comprises receiving the command at a client computer from a user.</i></p> <p>See analysis of portion [16.1].</p>
<p>[33.0] A data processing apparatus, comprising:</p>	<p>[33.0] <i>A data processing apparatus, comprising:</i></p> <p>See analysis of portions [1.0] and [17.0]. Kiuchi teaches installing and using the C-HTTP proxy software on a firewall. A firewall is a “data processing apparatus.”</p> <p>Thus, Kiuchi teaches a “data processing apparatus” as recited in the claim.</p>
<p>[33.1] a processor, and</p>	<p>[33.1] <i>a processor, and</i></p> <p>As analyzed in portion [33.0], Kiuchi teaches installing and using the C-HTTP proxy software on a firewall. It is understood that a firewall includes a processor.</p> <p>Thus, Kiuchi teaches a “processor” as recited in the claim.</p>
<p>[33.2] memory storing computer executable instructions which,</p>	<p>[33.2] <i>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</i></p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	See analysis of portions [1.0], [17.0] and [17.1].
[33.3] receiving a secure domain name;	[33.3] <i>receiving a secure domain name;</i> See analysis of portion [1.1].
[33.4] sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	[33.4] <i>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</i> See analysis of portions [1.2a]–[1.2b].
[33.5] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	[33.5] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i> See analysis of portion [1.3].

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>[33.6] sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>[33.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
<p>[34.0] The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:</p>	<p>[34.0] <i>The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 33.</p>
<p>[34.1] receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and</p>	<p>[34.1] <i>receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and</i></p> <p>See analysis of portions [2.1a]–[2.1b].</p>
<p>[34.2] automatically generating a secure domain name corresponding to the non-secure domain name.</p>	<p>[34.2] <i>automatically generating a secure domain name corresponding to the non-secure domain name.</i></p> <p>See analysis of portion [2.2].</p>
<p>[35.0] The apparatus of claim</p>	<p>[35.0] <i>The apparatus of claim 33,</i></p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)
33,	As analyzed above, Kiuchi teaches all of the limitations of claim 33.
[35.1] wherein the response message contains provisioning information for the virtual private network.	[35.1] <i>wherein the response message contains provisioning information for the virtual private network.</i> See analysis of portion [4.1].
[36.0] The apparatus of claim 35,	[36.0] <i>The apparatus of claim 35,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 33.
[36.1] wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.	[36.1] <i>wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.</i> See analysis of portions [5.1]–[5.2].
[37.0] The apparatus of claim 35,	[37.0] <i>The apparatus of claim 35,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 35.
[37.1] wherein the virtual private network is based on inserting into at least one data packet at least one data value	[37.1] <i>wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.</i> See analysis of portion [6.1].

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.1: Claims 1-6, 8-10, 12-22, 24-26, 28-37 & 39-40 are anticipated by Kiuchi under 35 U.S.C. § 102(b)</p>
<p>representing a predetermined level of service associated with the virtual private network.</p>	
<p>[39.0] The apparatus of claim 35,</p>	<p>[39.0] <i>The apparatus of claim 35,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 35.</p>
<p>[39.1] wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</p>	<p>[39.1] <i>wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.</i> See analysis of portion [8.1].</p>
<p>[40.0] The apparatus of claim 35,</p>	<p>[40.0] <i>The apparatus of claim 35,</i></p>
<p>[40.1] wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.</p>	<p>[40.1] <i>wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.</i> See analysis of portions [9.1a]–[9.1b].</p>

EXHIBIT E-2
Kiuchi

Section 2 – Obviousness

Chart E-2.2: Detailed support for Proposed Rejection #6, showing that claims 3 and 19 are obvious over Kiuchi in view of Masys under 35 U.S.C. § 103.

Daniel R. Masys & Dixie B. Baker, “Protecting Clinical Data on Web Client Computers: the PCASSO Approach,” Proceedings of the AMIA '98 Annual Symposium, Orlando, FL (Nov. 7-11, 1998). (“Masys”).

Masys is a printed publication published more than one year before the '180 Patent's earliest effective priority date of Apr. 26, 2000 and is prior art under 35 U.S.C. § 102(b). Masys is attached as Exhibit D-9.

Reasons to Combine Kiuchi and Masys

As shown in the following analysis, Kiuchi and Masys together teach all of the limitations of claims 3 and 19. Thus, there are no substantive differences between the features taught by the prior art and the limitations recited in claims 3 and 19. Accordingly, it would have been well within the ability of a person of ordinary skill in the art to combine the features of Kiuchi and Masys.

As shown in the analysis of Kiuchi above in Section 1 – Anticipation, Kiuchi generally discloses a network architecture for securing web browser communication sessions between hospitals over the Internet. Masys similarly discloses software for securing web browser communication sessions between hospitals over the Internet. Thus, Kiuchi and Masys are directed to similar network security technologies and environments.

It would have been obvious to one of skill in the art, before the filing of the '180 patent, to combine the Kiuchi network architecture with the additional techniques disclosed in Masys because the combination is merely the use of known techniques (as shown in Masys) to improve the similar Kiuchi system in the same way that these known techniques improve the Masys system. For example, combining the transparent encryption of Kiuchi with Masys' convenient one-click icon action for launching a session would further simplify the Kiuchi system for users. Thus, the combination would further improve the ease-of-use of Kiuchi's secure network.

Additionally, it would have been obvious to combine Kiuchi and Masys because the combination of known elements accordingly to known methods merely produces a predictable result. For example, combining the transparent encryption of Kiuchi with the icon-based application launch taught by Masys results in the predictable result of a secure network connection that may be launched by clicking on an icon. Those of skill in the art would have recognized that this predictable benefit would be available by incorporating icon-based launching into Kiuchi's system in the way suggested by Masys.

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.2: Claims 3 & 19 are obvious over Kiuchi in view of Masys under 35 U.S.C. § 103
[3.0] The method according to claim 2,	<p>[3.0] <i>The method according to claim 2</i></p> <p>As analyzed above, Kiuchi teaches all of the limitations of claim 2.</p>
[3.1] wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.	<p>[3.1] <i>wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.</i></p> <p>As explained in portion [1.4b], Kiuchi discloses the establishment of a virtual private network communication link. Kiuchi discloses that the established virtual private network uses HTTP as the communication protocol.</p> <p>Kiuchi further teaches that one of the advantages of HTTP is that it allows for the use of graphical interfaces based on hypertext: “Using HTTP and Hypertext Markup Language (HTML), distributed multimedia information systems with user-friendly graphical interfaces based on hypertext can be easily developed.” (Kiuchi at p. 67, emphasis added.)</p> <p>Predetermined icons are one example of a graphical interface based on hypertext.</p> <p>Similar to Kiuchi, Masys discloses a system for securing communications at computers used to access health care information. Specifically, Masys discloses running a Patient Centered Access to Secure Systems Online (PCASSO) program by selecting an icon to run a Supplemental Protection for the Client Environment (SPiCE) program:</p> <p style="padding-left: 40px;">The SPiCE code will be made available to all PCASSO users, and the installation will be configured such that <i>the user will "click" on an icon on the desktop to launch SPiCE.</i> SPiCE then will establish an anonymous SSL session with the PCASSO server to download the client's signature file, which will be used in</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.2: Claims 3 & 19 are obvious over Kiuchi in view of Masys under 35 U.S.C. § 103</p>
	<p>performing the environment integrity check. Assuming the environment checks "clean," <i>SPiCE will then launch the PCASSO application itself.</i></p> <p>(Masys at 369, emphasis added.)</p> <p>Masys further describes how SPiCE and PCASSO enable a secure communication link:</p> <p>The client is provided <i>encryption services that implement authentication and end-to-end confidentiality.</i> These encryption services prevent lower-layer malicious network protocols or device drivers from eavesdropping on data as they are exchanged between the Java Virtual Machine and the network interface.</p> <p>(Masys at 368, emphasis added.)</p> <p>SPiCE is designed to provide a continuous series of analyses that attempt to verify the integrity of the client operating environment and bound the type of activity that can occur during the client session. Two complementary security services are provided by SPiCE for the PCASSO client: operating environment Integrity Analysis and active monitoring Intrusion Detection.</p> <p>...</p> <p>Once the integrity of the SPiCE client is verified, SPiCE can begin to provide continuous monitoring to detect and respond to activity that is inconsistent with the PCASSO client's security requirements.</p> <p>(Masys at 369.)</p> <p>Thus, Kiuchi and Masys render obvious that "the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display," as recited by the claim.</p>
<p>[19.0] The computer-</p>	<p>[19.0] <i>The computer-readable medium according to claim 18,</i></p>

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.2: Claims 3 & 19 are obvious over Kiuchi in view of Masys under 35 U.S.C. § 103
readable medium according to claim 18,	As analyzed above, Kiuchi teaches all of the limitations of claim 18.
[19.1] wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.	[19.1] <i>wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.</i> See analysis of portion [3.1].

EXHIBIT E-2
Kiuchi

Chart E-2.3: Detailed support for Proposed Rejection #7, showing that claims 7, 23 and 38 are obvious over Kiuchi in view of Martin under 35 U.S.C. § 103.

David M. Martin, “A Framework for Local Anonymity in the Internet,” Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998) (“Martin”).

Martin is a printed publication published before the ’180 Patent’s earliest priority date of Oct. 30, 1998 and is at least prior art under 35 U.S.C. § 102(a). Martin is attached as Exhibit D-5.

Reasons to Combine Kiuchi and Martin

As shown in the following analysis, Kiuchi and Martin teach all of the limitations of claim 7. Thus, there are no substantive differences between the features taught by the prior art and the limitations recited in claim 7. Accordingly, it would have been well within the ability of a person of ordinary skill in the art to combine the features of Kiuchi and Martin.

As shown in the analysis of Kiuchi above in Section 1 – Anticipation, Kiuchi generally discloses a network architecture for securing network communications against interception by transparently encrypting packets. Martin generally discloses a network architecture for securing network communications against interception by anonymizing the source and destination of packets. Thus, Kiuchi and Martin are directed to similar network security architectures and technologies.

It would have been obvious to one of skill in the art, before the filing of the ’180 patent, to combine the Kiuchi network architecture with the additional techniques disclosed in Martin because the combination is merely the use of known techniques (as shown in Martin) to improve the similar Kiuchi system in the same way that these known techniques improve the Martin system. For example, with respect to claim 7, combining the transparent encryption of Kiuchi with the anonymized network addresses as taught by Martin would allow the Kiuchi network to prevent eavesdroppers from seeing not only the content of communications between two parties, but also *who* those parties were. Thus, the combination would further improve the security of the Kiuchi proxy architecture.

Additionally, it would have been obvious to combine Kiuchi and Martin because the combination of known elements accordingly to known methods merely produces a predictable result. For example, with respect to claim 7, combining the transparent encryption of Kiuchi with the anonymized network addresses as taught by Martin results in the predictable result of a network that provides both transparent packet encryption and anonymized endpoint addresses. Those of skill in the art would have recognized that this predictable benefit would be available by incorporating indirect connection addressing into Kiuchi’s client-side and server-side proxy in the way suggested by Martin.

EXHIBIT E-2
Kiuchi

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-2.2: Claims 7, 23 and 38 are obvious over Kiuchi in view of Martin under 35 U.S.C. § 103</p>
<p>[7.0] The method according to claim 4,</p>	<p>[7.0] <i>The method according to claim 4</i> As analyzed above, Kiuchi teaches all of the limitations of claim 4.</p>
<p>[7.1] wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</p>	<p>[7.1] <i>wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</i></p> <p>Martin teaches establishing the virtual private network communication link by creating an network address hopping regime between a first computer and a second computer:</p> <p style="padding-left: 40px;">Let A_{IP} be the set of anonymous IP addresses in the lanon, $PORT = \{0,1, \dots, 2^{16} - 1\}$ be the set of possible port numbers, and $A_{TCP} = A_{IP} \times PORT$ be the set of all possible TCP endpoint connection identifiers. Each such identifier is called an <i>anonymous TCP address</i>. A lanon client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random subject to lanon uniqueness and application-specific constraints. Randomly choosing the source label hides the node's identity from external (and internal) observers.</p> <p>(Martin at 9.)</p> <p>Choosing one of the source addresses “at random” shows establishing the virtual private network communication link through pseudorandomly changing computer network addresses as recited by the claim.</p> <p>One of skill in the art would have been motivated to combine Martin’s IP hopping scheme with Kiuchi’s secure, closed network in order to further provide anonymity protection to the network participants, as described in Martin.</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.2: Claims 7, 23 and 38 are obvious over Kiuchi in view of Martin under 35 U.S.C. § 103
[23.0] The computer-readable medium according to claim 20,	[23.0] <i>The computer-readable medium according to claim 20,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 20.
[23.1] wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.	[23.1] <i>wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</i> See analysis of portion [7.1].
[38.0] The apparatus of claim 35,	[38.0] <i>The apparatus of claim 35,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 35.
[38.1] wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change	[38.1] <i>wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.</i> See analysis of portion [7.1].

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.2: Claims 7, 23 and 38 are obvious over Kiuchi in view of Martin under 35 U.S.C. § 103
computer network addresses in packets transmitted between a first computer and a second computer.	

EXHIBIT E-2
Kiuchi

Chart E-2.4: Detailed support for Proposed Rejection #8, showing that claims 11, 27, and 41 are obvious over Kiuchi alone under 35 U.S.C. § 103.

U.S. Patent No. 7,188,180*	Chart E-2.4: Claims 11, 27 & 41 are obvious over Kiuchi alone under 35 U.S.C. § 103
[11.0] The method according to claim 1,	[11.0] <i>The method according to claim 1,</i> As analyzed above, Kiuchi teaches all of the limitations of claim 1.
[11.1] wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.	[11.1] <i>wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.</i> In view of Kiuchi’s disclosure of a secure domain name (portion [1.1]) that is different from a conventional DNS name (portion [2.1b]), a person of ordinary skill in the art would have considered the use of a top level domain name that includes .scom, .snet, .sorg, .sedu, .smil, or .sgov to be a matter of mere design choice. Design choice is “an acceptable rationale for an obviousness rejection when a claimed product merely arranges known elements in a configuration recognized as functionally equivalent to a known configuration.” <i>See, Ex parte Gunasekar</i> , Appeal 2009-008345 in 10/903,590 (BPAI 2011). Since Kiuchi teaches secure domain names that correspond to conventional domain names and since .com, .net, .org, .edu, and .gov are character combinations commonly known to represent top level domain names, arranging the known top level domain name character combinations with the additional known character “s” to abbreviate the descriptive term “security” is an obvious design choice. Thus, the method of claim 1 wherein a secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil, or .sgov would have been obvious in view of Kiuchi.
[27.0] The	[27.0] <i>The computer-readable medium according to claim 17,</i>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-2
Kiuchi

U.S. Patent No. 7,188,180*	Chart E-2.4: Claims 11, 27 & 41 are obvious over Kiuchi alone under 35 U.S.C. § 103
computer-readable medium according to claim 17,	As analyzed above, Lendenmann teaches all of the limitations of claim 17.
[27.1] wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.	[27.1] <i>wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.</i> See analysis of portion [11.1].
[41.0] The apparatus of claim 33,	[41.0] <i>The apparatus of claim 33,</i> As analyzed above, Lendenmann teaches all of the limitations of claim 33.
[41.1] wherein the secure domain name has a top-level domain name that includes one of scom, .snet, .sorg, .sedu, smil or .sgov.	[41.1] <i>wherein the secure domain name has a top-level domain name that includes one of scom, .snet, .sorg, .sedu, smil or .sgov.</i> See analysis of portion [11.1].

–End–

Exhibit E3

Claim charts applying Solana as a primary reference to the '180 patent.

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

EXHIBIT E-3
Solana

Contents

Chart E-3.1: Detailed support for Proposed Rejection #9, showing that claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)..... 2

EXHIBIT E-3
Solana

Anticipation

Chart E-3.1: Detailed support for Proposed Rejection #9, showing that claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b).

Solana is “Flexible Internet Secure Transactions Based on Collaborative Domains,” by Eduardo Solana and Jürgen Harms, Security Protocols Workshop 1997: 37-51.

Solana is a publication that was publicly available more than one year before the ’180 Patent’s earliest possible priority date of Oct. 30, 1998 and is prior art under 35 U.S.C. §102(b). A copy of Solana is attached as Exhibit D-3.

As potentially helpful guidance in giving the claims the broadest reasonable interpretation consistent with the specification, the following analysis makes occasional reference to the Patent Owner’s prior characterizations of the claims in the first reexamination, and to the claim interpretation from prior litigation involving the ’180 patent:

- Reexamination of US 7,188,180, Control No. 95/001,270, Patent Owner Response filed May 24, 2010 [*hereinafter* “Patent Owner Response”]. A copy of the Patent Owner Response is included in Exhibit B-3.
- *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009) [*hereinafter* “E.D. Tex. Order”]. A copy of the E.D. Tex. Order is attached as Exhibit B-4.

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
<p>[1.0] A method for accessing a secure computer network address, comprising steps of:</p>	<p>[1.0] <i>A method for accessing a secure computer network address, comprising steps of:</i></p> <p>Solana teaches a method for accessing a secure computer network address by providing end-to-end confidentiality of communications:</p> <p>End-to-end confidentiality. According to the characteristics</p>

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-3
Solana

U.S. Patent No. 7,188,180*	Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)
	<p>of the transaction and the principals involved, we propose two alternatives to achieve end-to-end confidentiality using domain collaborations.</p> <p>(Solana at 45.)</p> <p>Solana further teaches providing a transparent secure gateway service:</p> <p>As shown in this paper, domain granularity allows for both <i>transparent secure gatewaying between domains and end-to-end secure transactions</i>, and prevents the management problems related to a global structure of user certificates.</p> <p>(Solana at 48, emphasis added.)</p> <p>Solana that these end-to-end security features are provided via data encryption:</p> <p>Secure, domain-based, end-to-end transactions. The combination of intra-domain (local keys) and inter domain (global keys) <i>encryptions results in end-to-end confidentiality</i> and authentication.</p> <p>(Solana at 42, emphasis added.)</p> <p>Solana further teaches that engaging in the secure communications may require authorization for access by rejecting unauthenticated requests:</p> <p>If the destination DBS [Domain Border System] has firewall functionality, <i>it may reject transactions coming from unauthenticated domains</i>.</p> <p>(Solana at 47, emphasis added.)</p> <p>It is understood that engaging in secure communication, such as by encrypting transactions, involves “accessing a secure computer network address” as claimed.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10.)</p> <p>Thus, Solana teaches a “method for accessing a secure computer network address” as claimed.</p>
<p>[1.1] receiving a secure domain name;</p>	<p>[1.1] <i>receiving a secure domain name</i></p> <p>Solana discloses receiving a secure domain name.</p> <p>For example, Solana teaches that a Directory Service stores computer and domain naming information, along with their associated network addresses:</p> <p><i>A coordinated, global Directory Service (DS) holding naming information</i> and especially certificates that securely bind domains to their public keys is also required and constitutes the cryptographic support for inter-domain transactions. As mentioned, existing naming infrastructures (DNS-sec, X.509) might be used for this purpose.</p> <p>A well defined convention establishing an Uniform Naming Information (UNI) is also needed to designate principals and domains globally and unequivocally as, for instance, a common name, an E-mail address, or a <i>network address</i>. Note that this information <i>may also be published in the Directory Service</i>.</p> <p>(Solana at 43, emphasis added.)</p> <p>As noted above, the information may be stored in an “X.509” infrastructure. The naming information received by and stored in the global Directory Service (DS) includes a “secure domain name” as recited in the claim.</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the patent owner asserts that the phrase “secure domain name” refers to a name that “cannot be resolved by a conventional domain name service.” (Patent Owner Response at 6.)</p> <p>In addition, a federal court interpreted the phrase “secure domain name” to refer to a “domain name that corresponds to a secure computer network address.” (E.D. Tex. Opinion at 31.) The court interpreted a secure computer network address to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (<i>Id.</i> at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10)</p> <p>Thus, Solana teaches “receiving a secure domain name” as recited in the claim.</p>
<p>[1.2a] sending a query message to a secure domain name service, [1.2b] the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[1.2a] <i>sending a query message to a secure domain name service</i></p> <p>Solana teaches sending a query message to a secure domain name service.</p> <p>Specifically, Solana discloses sending a query to the global Directory Service (DS):</p> <p style="padding-left: 40px;">The initiator generates the same header as in the precedent case (Session Key + responder UNI) and then <i>issues a DS query</i> to obtain the destination domain public key for header encryption. Finally, the whole packet together with the decryption information is submitted directly to the responder.</p> <p>(Solana at 46, emphasis added.)</p> <p>As analyzed above in portion [1.0], Solana teaches that the global Directory Service may be, for example, an X.509 naming infrastructure instead of a conventional domain name service:</p> <p style="padding-left: 40px;">A coordinated, global Directory Service (DS) holding naming</p>

EXHIBIT E-3
Solana

U.S. Patent No. 7,188,180*	Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)
	<p>information and especially certificates that securely bind domains to their public keys is also required and constitutes the cryptographic support for inter-domain transactions. As mentioned, existing naming infrastructures (DNS-sec, X.509) <i>might be used for this purpose.</i></p> <p>(Solana at 43, emphasis added.)</p> <p>Thus, the query issued to the global Directory Service (DS) is a “query message to a secure domain name service.”</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserts that a “secure domain name service” is a name service that “is different from a conventional domain name service.” (Patent Owner Response at 8.)</p> <p>Thus, Solana teaches “sending a query message to a secure domain name service” as claimed.</p> <hr/> <p>[1.2b] <i>the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name</i></p> <p>Solana teaches that the global Directory Service (DS) is the repository for network address information:</p> <p><i>A coordinated, global Directory Service (DS) holding naming information</i> and especially certificates that securely bind domains to their public keys is also required and constitutes the cryptographic support for inter-domain transactions. As mentioned, existing naming infrastructures (DNS-sec, X.509) might be used for this purpose.</p> <p>A well defined convention establishing an Uniform Naming Information (UNI) is also needed to designate principals and domains globally and unequivocally as, for instance, a common name, an E-mail address, or a <i>network address</i>. Note that this information <i>may also be published in the Directory Service.</i></p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>(Solana at 43, emphasis added.)</p> <p>Thus, it is understood that the query message sent to the global Directory Service is a request for the network address of a requested destination.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (Id. at 10.)</p> <p>Thus, Solana teaches “the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.3] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name;</p>	<p>[1.3] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name</i></p> <p>Solana discloses receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.</p> <p>Specifically, Solana teaches that network addresses are published in the global Directory Service (DS):</p> <p style="padding-left: 40px;">A well defined convention establishing an Uniform Naming Information (UNI) is also needed to designate principals and domains globally and unequivocally as, for instance, a common name, an E-mail address, or a <i>network address</i>. Note that this information <i>may also be published in the Directory Service</i>.</p> <p>(Solana at 43, emphasis added.)</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>As analyzed above in portions [1.2a]–[1.2b], Solana teaches sending a query to the global Directory Service (DS) is the repository for network address information. It is understood that the global Directory Service (DS) responds with the requested information, such as the secure computer network address corresponding to the provided secure domain name.</p> <p>Thus, Solana teaches “receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.4a] and sending an access request message to the secure computer network address [1.4b] using a virtual private network communication link.</p>	<p>[1.4a] and sending an access request message to the secure computer network address</p> <p>Solana teaches sending an access request message to the secure computer network address. Specifically, Solana teaches that an initiator sends an access request message to communicate with a responder:</p> <ol style="list-style-type: none"> 1. The initiator generates the same header as in the precedent case (Session Key + responder UNI) and then issues a DS query to obtain the destination domain public key for header encryption. Finally, <i>the whole packet together with the decryption information is submitted directly to the responder.</i> <p>(Solana at 46, emphasis added.)</p> <p>The packet submitted to the responder at the address provided in response to the DS query is “an access request message to the secure computer network address.”</p> <p>Thus, Solana teaches “sending an access request message to the secure computer network address” as recited in the claim.</p> <hr/> <p>[1.4b] using a virtual private network communication link.</p> <p>Solana teaches that the communication link established between the initiator and responder is a virtual private network.</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>For example, Solana teaches protecting an organization with a virtual private network:</p> <p style="padding-left: 40px;">This means, organizations concerned by security issues conceive strong internal security policies and interact with the Internet through very restrictive firewalls or by means of well-protected <i>Virtual Private Networks (VPN)</i>.</p> <p>(Solana at 38, emphasis added.)</p> <p>Solana further discloses that the initiator encrypts the contents of the transaction sent to the responder:</p> <p style="padding-left: 40px;">1. The <i>initiator generates a session key for encrypting transaction contents</i> and creates a header containing the session key and the UNI of the responder. This header is encrypted with the source domain public key and sent to the source DBS together with the transaction core. Additional decryption information (DI) - such as the decryptor UNI and encryption parameters - is sent in the clear to make possible the decryption process.</p> <p>(Solana at 45, emphasis added.)</p> <p>By encrypting communications between the initiator and responder, Solana teaches providing a “virtual private network” as recited in the claim.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (E.D. Tex. Opinion at 10.)</p> <p>Thus, Solana teaches sending an access request message “using a virtual private network communication link” as recited in the claim.</p>
<p>[4.0] The method according to claim</p>	<p>[4.0] <i>The method according to claim 1</i></p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
<p>1,</p>	<p>As analyzed above, Solana teaches all of the limitations of claim 1.</p>
<p>[4.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[4.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>Solana discloses that the global Directory Service (DS) is the repository for encryption keys, and that the initiator’s request to the global Directory Service (DS) is (in part) to obtain encryption key information:</p> <p style="padding-left: 40px;">1. The initiator generates the same header as in the precedent case (Session Key + responder UNI) and then <i>issues a DS query to obtain the destination domain public key for header encryption</i>. Finally, the whole packet together with the decryption information is submitted directly to the responder.</p> <p>(Solana at 46, emphasis added.)</p> <p>The destination domain public key for header encryption is “provisioning information for the virtual private network” as recited in the claim. It is understood that the global Directory Service (DS) provides the requested encryption key in the response message.</p> <p>Thus, Solana teaches that “the response message contains provisioning information for the virtual private network” as recited in the claim.</p>
<p>[10.0] The method according to claim 1,</p>	<p>[10.0] <i>The method according to claim 1,</i></p> <p>As analyzed above, Solana teaches all of the limitations of claim 1.</p>
<p>[10.1] wherein the virtual private network includes the Internet.</p>	<p>[10.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>Solana teaches that the virtual private network includes the Internet. For example, the title of Solana’s paper is “Flexible Internet Secure Transactions Based on Collaborative Domains.”</p> <p>Solana further teaches that the disclosed technologies for securing communications between the initiator and responder are designed to secure Internet transactions:</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>This paper is structured in two major parts. The first one describes the benefits of introducing domains for the provision of security services by comparing them to their user-based counterparts; the second part focuses on the architectural needs of the collaborative domains and explains how the elements of this architecture interact in order to <i>deliver security services to Internet transactions</i>.</p> <p>(Solana at 41, emphasis added.)</p> <p>Thus, Solana teaches the method of claim 1 wherein the virtual private network includes the Internet.</p>
<p>[12.0] The method according to claim 1,</p>	<p>[12.0] <i>The method according to claim 1,</i></p> <p>As analyzed above, Solana teaches all of the limitations of claim 1.</p>
<p>[12.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[12.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i></p> <p>As analyzed above at portion [1.4a], Solana teaches the access request message of claim 1. As analyzed above at portion [1.0], Solana also teaches a “secure computer network address,” such as the network address of the responder.</p> <p>Solana further teaches that the responder may be server providing transactions such as a World Wide Web (WWW) or e-mail service:</p> <p>For simplicity, we divide the principals into two categories: initiators (the Email sender, the WWW client, or the rlogin user) and <i>responders</i> (the E-mail recipient, <i>the WWW server</i>, or the rlogin daemon).</p> <p>(Solana at 42, emphasis added.)</p> <p>Since the present work is in an early stage, its application, so far, has only been analysed for some very specific Internet transactions - <i>such as the WWW</i> and the E-mail.</p> <p>(Solana at 49, emphasis added.)</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>It is understood that, for example, WWW transactions involve requests for information stored at the responder server, such as a web page.</p> <p>Thus, Solana teaches “the access request message contains a request for information stored at the secure computer network address.”</p>
<p>[14.0] The method of claim 1,</p>	<p>[14.0] <i>The method of claim 1,</i></p> <p>As analyzed above, Solana teaches all of the limitations of claim 1.</p>
<p>[14.1] performed by a software module.</p>	<p>[14.1] <i>performed by a software module.</i></p> <p>Solana teaches that each of the method steps recited in claim 1 is performed by a software module. For example, Solana discloses that the steps may be performed by a World Wide Web (WWW) client as the initiator, and a World Wide Web (WWW) server as the responder:</p> <p style="padding-left: 40px;">For simplicity, we divide the principals into two categories: <i>initiators</i> (the Email sender, <i>the WWW client</i>, or the rlogin user) and <i>responders</i> (the E-mail recipient, <i>the WWW server</i>, or the rlogin daemon).</p> <p>(Solana at 42, emphasis added.)</p> <p>It is understood that a WWW client and WWW server are software modules.</p> <p>Thus, Solana teaches the method “performed by a software module” as recited in the claim.</p>
<p>[17.0] A computer-readable storage medium, comprising:</p>	<p>[17.0] <i>A computer-readable storage medium, comprising:</i></p> <p>Solana discloses that the steps may be performed by a World Wide Web (WWW) client as the initiator, and a World Wide Web (WWW) server as the responder:</p> <p style="padding-left: 40px;">For simplicity, we divide the principals into two categories: <i>initiators</i> (the Email sender, <i>the WWW client</i>, or the rlogin user) and <i>responders</i> (the E-mail recipient, <i>the WWW server</i>,</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
	<p>or the rlogin daemon).</p> <p>(Solana at 42, emphasis added.)</p> <p>It is understood that a WWW client and WWW server are each a computer with at least one computer-readable storage medium.</p> <p>Thus, Solana teaches a “computer-readable storage medium” as recited in the claim.</p>
<p>[17.1] a storage area; and</p>	<p>[17.1] <i>a storage area; and</i></p> <p>See analysis of portion [17.0]. The computer-readable <i>storage medium</i> includes a “storage area.”</p>
<p>[17.2] computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>[17.2] <i>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</i></p> <p>See analysis of portions [1.0] and [17.0]. It is understood that the methods taught by Solana are “computer-readable instructions” for execution on, for example, the WWW client and WWW server.</p> <p>Thus, Solana teaches “computer-readable instructions for a method for accessing a secure computer network address,” recited in the claim.</p>
<p>[17.3] receiving a secure domain name;</p>	<p>[17.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[17.4] sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain</p>	<p>[17.4] <i>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>

EXHIBIT E-3
Solana

U.S. Patent No. 7,188,180*	Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)
name;	
[17.5] receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	<p>[17.5] <i>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>
[17.6] sending an access request message to the secure computer network address using a virtual private network communication link.	<p>[17.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
[20.0] The computer-readable medium according to claim 17,	<p>[20.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Solana teaches all of the limitations of claim 17.</p>
[20.1] wherein the response message contains provisioning information for the virtual private network.	<p>[20.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>See analysis of portion [4.1].</p>
[26.0] The computer-readable medium according to claim 17,	<p>[26.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Solana teaches all of the limitations of claim 17.</p>
[26.1] wherein the virtual private network includes	<p>[26.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>See analysis of portion [10.1].</p>

EXHIBIT E-3
Solana

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)</p>
<p>the Internet.</p>	
<p>[28.0] The computer readable medium of claim 17,</p>	<p>[28.0] <i>The computer readable medium of claim 17,</i> As analyzed above, Solana teaches all of the limitations of claim 17.</p>
<p>[28.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[28.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i> See analysis of portion [12.1].</p>
<p>[30.0] The computer-readable medium according to claim 17,</p>	<p>[30.0] <i>The computer-readable medium according to claim 17,</i> As analyzed above, Solana teaches all of the limitations of claim 20.</p>
<p>[30.1] wherein the method is performed by a software module.</p>	<p>[30.1] <i>wherein the method is performed by a software module.</i> See analysis of portion [14.1].</p>
<p>[33.0] A data processing apparatus, comprising:</p>	<p>[33.0] <i>A data processing apparatus, comprising:</i> See analysis of portions [1.0] and [17.0]. Solana teaches computers such as a WWW server and a WWW client. A computer is a “data processing apparatus.” Thus, Solana teaches a “data processing apparatus” as recited in the claim.</p>
<p>[33.1] a processor, and</p>	<p>[33.1] <i>a processor, and</i> As analyzed in portion [33.0], Solana teaches computers such as a WWW server and a WWW client. It is understood that a computer includes a processor. Thus, Solana teaches a “processor” as recited in the claim.</p>

EXHIBIT E-3
Solana

U.S. Patent No. 7,188,180*	Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)
<p>[33.2] memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>[33.2] <i>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</i></p> <p>See analysis of portions [1.0], [17.0] and [17.1].</p>
<p>[33.3] receiving a secure domain name;</p>	<p>[33.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[33.4] sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[33.4] <i>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>
<p>[33.5] receiving from the secure domain name service a response message containing the secure</p>	<p>[33.5] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>

EXHIBIT E-3
Solana

U.S. Patent No. 7,188,180*	Chart E-3.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are anticipated by Solana under 35 U.S.C. § 102(b)
computer network address corresponding to the secure domain name; and	
[33.6] sending an access request message to the secure computer network address using a virtual private network communication link.	[33.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i> See analysis of portions [1.4a]–[1.4b].
[35.0] The apparatus of claim 33,	[35.0] <i>The apparatus of claim 33,</i> As analyzed above, Solana teaches all of the limitations of claim 33.
[35.1] wherein the response message contains provisioning information for the virtual private network.	[35.1] <i>wherein the response message contains provisioning information for the virtual private network.</i> See analysis of portion [4.1].

–End–

Exhibit E4

Claim charts applying Schimpf and Rosenberry as references to the '180 patent.

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

EXHIBIT E-4
Schimpf & Rosenberry

Contents

Chart E-4.1: Detailed support for Proposed Rejection #10, showing that claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103. 2

EXHIBIT E-4
Schimpf & Rosenberry

Anticipation

Chart E-4.1: Detailed support for Proposed Rejection #10, showing that claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103.

Schimpf is “Securing Web Access with DCE,” by Brian C. Schimpf, presented at Network and Distributed System Security, Feb. 10-11, 1997.

Rosenberry is UNDERSTANDING DCE by Ward Rosenberry, David Kenney, and Gerry Fisher (1993).

Schimpf is a publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of Oct. 30, 1998 and is prior art under 35 U.S.C. §102(b). A copy of Schimpf is attached as Exhibit D-7.

Rosenberry is a publication that was publicly available more than one year before the '180 Patent's earliest claimed priority date of Oct. 30, 1998 and is prior art under 35 U.S.C. §102(b). A copy of Rosenberry is attached as Exhibit D-8.

As potentially helpful guidance in giving the claims the broadest reasonable interpretation consistent with the specification, the following analysis makes occasional reference to the Patent Owner's prior characterizations of the claims in the first reexamination, and to the claim interpretation from prior litigation involving the '180 patent:

- Reexamination of US 7,188,180, Control No. 95/001,270, Patent Owner Response filed May 24, 2010 [*hereinafter* “Patent Owner Response”]. A copy of the Patent Owner Response is included in Exhibit B-3.
- *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009) [*hereinafter* “E.D. Tex. Order”]. A copy of the E.D. Tex. Order is attached as Exhibit B-4.

Reasons to Combine Schimpf and Rosenberry

Schimpf “describes work done to utilize the security services and infrastructure of the Open Software Foundation (OSF) Distributed Computing Environment (DCE) to secure Web accesses.”¹ Rosenberry is directed to explaining this same OSF DCE software architecture:

Understanding DCE fills a serious information gap that has emerged in the field of networked computing. On one side is the Distributed Computing Environment (DCE), an enormous software system from the Open Software Foundation (OSF) embodying some novel and complex concepts. On the other side stand potential

¹ Schimpf, Abstract.

EXHIBIT E-4
Schimpf & Rosenberry

purchasers, system administrators, application programmers, and end users, many of whom have little previous exposure to distributed computing. Before studying and mastering the various daemons, utilities, and programming libraries that make up DCE, newcomers must answer the basic questions “What are all these things?” and “What do they mean for me?”

In this book we try to answer those questions.²

Thus, it would have been obvious to one of ordinary skill in the art to combine the teachings of Schimpf and Rosenberry for at least the reason that Rosenberry is expressly directed to explaining the software architecture used in Schimpf.

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>[1.0] A method for accessing a secure computer network address, comprising steps of:</p>	<p>[1.0] <i>A method for accessing a secure computer network address, comprising steps of:</i></p> <p>Schimpf teaches a method for accessing a secure computer network address by securing access to Web documents and application servers:</p> <p>This paper describes work done to utilize the security services and infrastructure of the Open Software Foundation (OSF) Distributed Computing Environment (DCE) to secure Web accesses. This work was done as part of an Advanced Technology Offering (ATO) by the OSF Research Institute jointly with Gradient Technologies Inc. and other ATO sponsors. A practical implementation has been completed. These combined technologies <i>allow users to securely access both Web documents and application servers</i> from a variety of desktop systems using standard, of-the-shelf Web</p>

² Rosenberry at xix.

* In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The real party in interest reserves the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
	<p>browsers.</p> <p>(Schimpf, Abstract, emphasis added.)</p> <p>It is understood that securely accessing Web documents and application servers involves “accessing a secure computer network address.”</p> <p>Additionally, Schimpf states that “if the system is configured for privacy protection then <i>all data will be encrypted before transmission</i>, so a network technician with access to a network sniffer will not e able to observe Alice’s salary or telephone number.” (Schimpf at 107, emphasis added.)</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10.)</p> <p>Thus, Schimpf teaches a “method for accessing a secure computer network address” as claimed.</p>
<p>[1.1] receiving a secure domain name;</p>	<p>[1.1] <i>receiving a secure domain name</i></p> <p>Schimpf discloses receiving a secure domain name.</p> <p>For example, Schimpf teaches that a Secure Local Proxy (SLP) intercepts all requests from a web browser and determines whether a request is for normal Web access or for a special, secure access via a Distributed Computing Environment (DCE) remote procedure call (RPC):</p> <p>In addition to the browser, DCE runtime services are installed on the system, as is a component called <i>the Secure Local Proxy (SLP)</i>. The SLP <i>intercepts all HTTP requests from the browser</i> using a standard browser proxy mechanism. If</p>

EXHIBIT E-4
Schimpf & Rosenberry

U.S. Patent No. 7,188,180*	Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103
	<p>the request is <i>for a normal Web access the request is forwarded directly to the Web server</i> using HTTP. The SLP can be configured to forward the request to another proxy process if required. If, on the other hand, the request is <i>for a DCE-enabled Web access, determined by the presence of a DCE CDS object name in the URL</i>, the SLP locates an appropriate DCE-aware Web server to fulfill the request using DCE naming services. The SLP then “tunnels” the request to that server by <i>wrapping the HTTP request in a secure DCE RPC</i>.</p> <p>(Schimpf at 105, emphasis added.)</p> <p>It is understood that the presence of a DCE CDS object name in the URL, which triggers the secure DCE RPC, shows that the URL contains a secure domain name.</p> <p>For example, Rosenberry provides examples of DCE server names, which are not conventional domain names and could not be resolved by a conventional domain name service:</p> <p>Every resource in a cell has a unique name. Uniqueness is conveyed through the hierarchical nature of the names. Here are two examples of hierarchical names:</p> <pre>././service/qserver_1 ././service/qserver_2</pre> <p>(Rosenberry at 72.)</p> <p>Thus, Schimpf and Rosenberry together teach that the Secure Local Proxy (SLP) receives and recognizes that a URL contains a secure domain name that requires handling through a secure DCE remote procedure call.</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted the phrase “secure domain name” to refer to a “domain name that corresponds to a secure computer network address.” (E.D. Tex. Opinion at 31.) The court interpreted a secure computer network address</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
	<p>to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (<i>Id.</i> at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (<i>Id.</i> at 10)</p> <p>Thus, Schimpf teaches “receiving a secure domain name” as recited in the claim.</p>
<p>[1.2a] sending a query message to a secure domain name service, [1.2b] the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[1.2a] <i>sending a query message to a secure domain name service</i></p> <p>As analyzed above in portion [1.1], Schimpf teaches that the Secure Local Proxy (SLP) executes a secure remote procedure call (RPC).</p> <p>Rosenberry discloses that in executing a remote procedure call (RPC), the software executes stub code to handle certain tasks relating to the communication link:</p> <p style="padding-left: 40px;">At run time, RPC software—the stub code and RPC runtime libraries that exist on client and server hosts—converts data to the appropriate formats and <i>performs all communication between client and server.</i></p> <p>(Rosenberry at 42, emphasis added.)</p> <p>Rosenberry further teaches that one of the tasks of the stub code is to first determine the network address of the secure server by contacting a directory service:</p> <p style="padding-left: 40px;">The client stub code accepts the input arguments from the program. Then the client stub code calls routines from the RPC runtime library to find and communicate with the server. RPC runtime routines do the following:</p> <ul style="list-style-type: none"> • Determine which network transport (for example, TCP/IP or UDP/IP) to use for communication • <i>Search the directory service for the server’s host address</i> • <i>Connect to and transmit the remote procedure call to the server</i>

EXHIBIT E-4
Schimpf & Rosenberry

U.S. Patent No. 7,188,180*	Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103
	<p>(Rosenberry at 43, emphasis added.)</p> <p>Rosenberry teaches that the cell directory service (CDS) stores information about objects, such as network addresses:</p> <p>It is important to realize that CDS objects are just information about resources, not the resources themselves. A program cannot gain access to a file simply by opening the corresponding CDS object. But the program can use the address obtained from the CDS object to find the file. Similarly, an object entry for a printer might store information like “color graphics printer, floor 2, network address 130.124.97.7.” After getting this descriptive information (called object attributes) from CDS, a program can create a print request and spool it to the printer. Note that RPC takes care of getting the address information from CDS so the application doesn’t have to.</p> <p>(Rosenberry at 73.)</p> <p>Thus, the cell directory service (CDS) is a “secure domain name service.”</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserts that a “secure domain name service” is a name service that “is different from a conventional domain name service.” (Patent Owner Response at 8.)</p> <p>Thus, Schimpf and Rosenberry render obvious “sending a query message to a secure domain name service” as claimed.</p> <hr/> <p>[1.2b] <i>the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name</i></p> <p>Rosenberry teaches that a client contacts a cell directory service (CDS) to obtain address information for a name:</p>

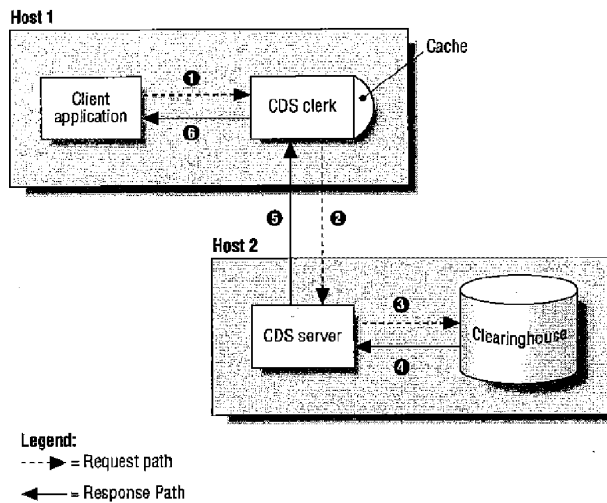
EXHIBIT E-4
Schimpf & Rosenberry

U.S. Patent No. 7,188,180* Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103

Figure 6-3 shows the interaction between a CDS client, clerk, server, and clearinghouse during a simple lookup.

- ❶ The client application on Host 1 sends a lookup request to the local clerk.
- ❷ The clerk checks its cache and, not finding the name there, contacts the server on Host 2.
- ❸ The server checks to see whether the name is in its clearinghouse.
- ❹ The name exists in the clearinghouse, so the server gets the requested information.
- ❺ The server returns the information to the clerk on Host 1.
- ❻ The clerk passes the requested data to the client application. The clerk also caches the information so that it does not have to contact a server the next time a client requests a lookup of that same name.

(Rosenberry at 80.)



Rosenberry Fig. 6-3.

As analyzed above in portion [1.2a], the cell directory service (CDS) is a “secure domain name service.” The address information returned by the cell directory service (CDS) is a “secure computer network address.”

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
	<p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that the Patent Owner asserted that a secure computer network address is an address that requires authorization for access or communication. See, for example, Patent Owner Response at 6 (stating that “the computers ... themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them.”).</p> <p>In addition, a federal court interpreted the phrase “secure computer network address” to refer to a “network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” (E.D. Tex. Opinion at 29.) The court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (Id. at 10.)</p> <p>Thus, Schimpf in view of Rosenberry teaches “the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name” as recited in the claim.</p>
<p>[1.3] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name;</p>	<p>[1.3] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name</i></p> <p>Rosenberry teaches that the cell directory service (CDS) returns a requested secure server’s corresponding secure network address:</p> <p>The DCE Directory Service stores the names of resources in the DCE. Resources include things like print servers, application servers, or other DCE services. <i>When given a name, the DCE Directory Service returns the unique network address of the named resource.</i> The Directory Service component that controls names inside cells is called the Cell Directory Service (CDS).</p> <p>(Rosenberry at 30-31, emphasis added.)</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
	<p>The Directory Service makes it possible to contact people and use resources such as disks, print queues, and servers anywhere in the network without knowing their physical location. The Directory Service is much like a telephone directory assistance service that provides a phone number when given a person's name. Given a unique name of a person, server, or other resource, the Directory Service can return the network address of that resource along with other information associated with the name.</p> <p>The Directory Service provides DCE distributed applications with a place to store and find information about resources available in the distributed computing environment. Currently, a major use of the Directory Service is to provide DCE distributed application clients with a remote server's network address.</p> <p>(Rosenberry at 71.)</p> <p>Thus, Schimpf in view of Rosenberry teaches "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name" as recited in the claim.</p>
<p>[1.4a] and sending an access request message to the secure computer network address [1.4b] using a virtual private network communication link.</p>	<p>[1.4a] <i>and sending an access request message to the secure computer network address</i></p> <p>Schimpf teaches that the Secure Local Proxy (SLP) sends an access request message to the secure computer network address:</p> <p style="padding-left: 40px;">The SLP then "tunnels" the request to that server by wrapping the HTTP request in a secure DCE RPC.</p> <p>(Schimpf at 105.)</p> <p>Thus, Schimpf in view of Rosenberry teaches "sending an access request message to the secure computer network address" as recited in the claim.</p> <hr/> <p>[1.4b] <i>using a virtual private network communication link.</i></p> <p>Schimpf teaches that the request sent by the Secure Local Proxy (SLP) includes authorization information and authentication <i>plus</i> privacy (encryption) protection:</p>

EXHIBIT E-4
Schimpf & Rosenberry

U.S. Patent No. 7,188,180*	Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103
	<p>The SLP then “tunnels” the request to that server by wrapping the HTTP request in a secure DCE RPC. The SLP is therefore a DCE client. This will typically be an authenticated DCE interaction and <i>the proper DCE authorization information</i>, specifically a DCE PAC (privilege attribute certificate), <i>will be transferred with the request</i>. This DCE interaction can be configured to use either no security, authentication only or <i>authentication plus privacy (i.e., encryption) protection</i>. By choosing privacy protection the DCE RPC access between the SLP and the application server is encrypted prior to transmission in either direction, thus protecting the information exchanged from observers with access to network traffic.</p> <p>(Schimpf at 105.)</p> <p>Schimpf further teaches encrypting all traffic using the DES encryption standard:</p> <p style="padding-left: 40px;">Protocol transactions between clients and servers can be integrity-protected against modification in transit using MD5 or optionally <i>privacy-protected by encrypting all traffic</i> with DES.</p> <p>(Schimpf at 103.)</p> <p>By tunneling the request with authorization information over an authenticated, encrypted remote procedure call, the Secure Local Proxy (SLP) uses a “virtual private network communication link.”</p> <p>As evidence that this interpretation is within the broadest reasonable interpretation of a person of skill in the art, note that a federal court interpreted a virtual private network to be a “network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.” (E.D. Tex. Opinion at 10.)</p> <p>Thus, Schimpf in view of Rosenberry teaches sending an access request message “using a virtual private network communication link” as recited</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
	<p>in the claim.</p>
<p>[4.0] The method according to claim 1,</p>	<p>[4.0] <i>The method according to claim 1</i></p> <p>As analyzed above, Schimpf in view of Rosenberry render obvious all of the limitations of claim 1.</p>
<p>[4.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[4.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>As noted above in portion [1.2a], Rosenberry teaches that the cell directory service (CDS) provides a repository for any kind of information about a resource:</p> <p style="padding-left: 40px;">It is important to realize that CDS objects are just information about resources, not the resources themselves. A program cannot gain access to a file simply by opening the corresponding CDS object. But the program can use the address obtained from the CDS object to find the file. Similarly, an object entry for a printer might store information like “color graphics printer, floor 2, network address 130.124.97.7.” After getting this descriptive information (called object attributes) from CDS, a program can create a print request and spool it to the printer. Note that RPC takes care of getting the address information from CDS so the application doesn’t have to.</p> <p>(Rosenberry at 73.)</p> <p>It would have been obvious to one of skill in the art that the cell directory service (CDS) could also store and return provisioning information for the virtual private network.</p> <p>Thus, Schimpf in view of Rosenberry render obvious that “the response message contains provisioning information for the virtual private network” as recited in the claim.</p>
<p>[10.0] The method according to claim 1,</p>	<p>[10.0] <i>The method according to claim 1,</i></p> <p>As analyzed above, Schimpf in view of Rosenberry renders obvious all of the limitations of claim 1.</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>[10.1] wherein the virtual private network includes the Internet.</p>	<p>[10.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>Schimpf discloses accessing information over the Internet:</p> <p style="padding-left: 40px;">Internet tools, especially Web browsers and servers, are being widely used for information access.</p> <p>(Schimpf, Abstract.)</p> <p>Thus, Schimpf in view of Rosenberry renders obvious that “the virtual private network includes the Internet.”</p>
<p>[12.0] The method according to claim 1,</p>	<p>[12.0] <i>The method according to claim 1,</i></p> <p>As analyzed above, Schimpf in view of Rosenberry renders obvious all of the limitations of claim 1.</p>
<p>[12.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[12.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i></p> <p>Schimpf teaches that the combination of traditional Web browser with the DCE security and naming services. It is understood that requests from a Web browser are for information stored at the target server:</p> <p style="padding-left: 40px;">Bringing together Web access mechanisms with the DCE security and naming services creates a very powerful, scaleable and useful distributed information management environment. This is especially useful in an “intranet;” where access to information and resources is occurring within an organization or between cooperating organizations. In these cases user principals are known and their accesses can be authenticated and authorized. By using standard Web browsers as the client portion of the distributed application users are able to develop and deploy distributed applications much faster across a large scale, heterogeneous client population. Since all the software required to access any application is the browser and the infrastructure software, deployment and administration of the desktop client systems is significantly simplified.</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
	<p>(Schimpf at 103.)</p> <p>For example, Schimpf describes how a client requests information from an application server:</p> <p style="padding-left: 40px;">The architecture combining DCE and the Web accommodates a classic three-tier distributed processing model, where the client system requests information from an application server, which implements the appropriate business logic of the enterprise.</p> <p>(Schimpf at 104.)</p> <p>Schimpf further describes an example application server that simply returns a requested HTML document:</p> <p style="padding-left: 40px;">This second tier is where the application-specific processing is done. This can be as simple as <i>returning a requested HTML document</i> or can consist of complex accumulation and processing of data prior to presentation to the user.</p> <p>(Schimpf at 105.)</p> <p>Thus, Schimpf in view of Rosenberry render obvious that “the access request message contains a request for information stored at the secure computer network address.”</p>
<p>[14.0] The method of claim 1,</p>	<p>[14.0] <i>The method of claim 1,</i></p> <p>As analyzed above, Solana teaches all of the limitations of claim 1.</p>
<p>[14.1] performed by a software module.</p>	<p>[14.1] <i>performed by a software module.</i></p> <p>See analysis of the portions of claim 1. Schimpf’s web browser, Secure Local Proxy (SLP), and DCE servers are all software modules.</p> <p>Thus, Schimpf in view of Rosenberry renders obvious the method “performed by a software module” as recited in the claim.</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>[17.0] A computer-readable storage medium, comprising:</p>	<p>[17.0] <i>A computer-readable storage medium, comprising:</i></p> <p>Schimpf and Rosenberry are both generally directed to computer software.</p> <p>Thus, Schimpf and Rosenberry render obvious a “computer-readable storage medium” as recited in the claim.</p>
<p>[17.1] a storage area; and</p>	<p>[17.1] <i>a storage area; and</i></p> <p>See analysis of portion [17.0]. It would have been obvious to one of skill in the art to store the software of Schimpf and Rosenberry in a “storage area.”</p>
<p>[17.2] computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</p>	<p>[17.2] <i>computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:</i></p> <p>See analysis of portions [1.0] and [17.0].</p>
<p>[17.3] receiving a secure domain name;</p>	<p>[17.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[17.4] sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain</p>	<p>[17.4] <i>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>name;</p>	
<p>[17.5] receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>[17.5] <i>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>
<p>[17.6] sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>[17.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
<p>[20.0] The computer-readable medium according to claim 17,</p>	<p>[20.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Schimpf and Rosenberry render obvious all of the limitations of claim 17.</p>
<p>[20.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[20.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>See analysis of portion [4.1].</p>
<p>[26.0] The computer-readable medium according to claim 17,</p>	<p>[26.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Schimpf and Rosenberry render obvious all of the limitations of claim 17.</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>[26.1] wherein the virtual private network includes the Internet.</p>	<p>[26.1] <i>wherein the virtual private network includes the Internet.</i></p> <p>See analysis of portion [10.1].</p>
<p>[28.0] The computer readable medium of claim 17,</p>	<p>[28.0] <i>The computer readable medium of claim 17,</i></p> <p>As analyzed above, Schimpf and Rosenberry render obvious all of the limitations of claim 17.</p>
<p>[28.1] wherein the access request message contains a request for information stored at the secure computer network address.</p>	<p>[28.1] <i>wherein the access request message contains a request for information stored at the secure computer network address.</i></p> <p>See analysis of portion [12.1].</p>
<p>[30.0] The computer-readable medium according to claim 17,</p>	<p>[30.0] <i>The computer-readable medium according to claim 17,</i></p> <p>As analyzed above, Schimpf and Rosenberry render obvious all of the limitations of claim 20.</p>
<p>[30.1] wherein the method is performed by a software module.</p>	<p>[30.1] <i>wherein the method is performed by a software module.</i></p> <p>See analysis of portion [14.1].</p>
<p>[33.0] A data processing apparatus, comprising:</p>	<p>[33.0] <i>A data processing apparatus, comprising:</i></p> <p>See analysis of portions [1.0] and [17.0]. It is understood that a computer is a “data processing apparatus.”</p> <p>Thus, Schimpf and Rosenberry render obvious a “data processing apparatus” as recited in the claim.</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>[33.1] a processor, and</p>	<p>[33.1] <i>a processor, and</i></p> <p>It is understood that a computer includes a processor.</p> <p>Thus, Schimpf and Rosenberry render obvious a “processor” as recited in the claim.</p>
<p>[33.2] memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</p>	<p>[33.2] <i>memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:</i></p> <p>See analysis of portions [1.0], [17.0] and [17.1].</p>
<p>[33.3] receiving a secure domain name;</p>	<p>[33.3] <i>receiving a secure domain name;</i></p> <p>See analysis of portion [1.1].</p>
<p>[33.4] sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</p>	<p>[33.4] <i>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</i></p> <p>See analysis of portions [1.2a]–[1.2b].</p>

EXHIBIT E-4
Schimpf & Rosenberry

<p>U.S. Patent No. 7,188,180*</p>	<p>Chart E-4.1: Claims 1, 4, 10, 12, 14, 17, 20, 26, 28, 30, 33, & 35 are obvious over Schimpf in view of Rosenberry under 35 U.S.C. § 103</p>
<p>[33.5] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</p>	<p>[33.5] <i>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</i></p> <p>See analysis of portion [1.3].</p>
<p>[33.6] sending an access request message to the secure computer network address using a virtual private network communication link.</p>	<p>[33.6] <i>sending an access request message to the secure computer network address using a virtual private network communication link.</i></p> <p>See analysis of portions [1.4a]–[1.4b].</p>
<p>[35.0] The apparatus of claim 33,</p>	<p>[35.0] <i>The apparatus of claim 33,</i></p> <p>As analyzed above, Schimpf and Rosenberry render obvious all of the limitations of claim 33.</p>
<p>[35.1] wherein the response message contains provisioning information for the virtual private network.</p>	<p>[35.1] <i>wherein the response message contains provisioning information for the virtual private network.</i></p> <p>See analysis of portion [4.1].</p>

–End–

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:	7188180 .				
Filer:	David L. McCombs/Theresa O'Connor				
Attorney Docket Number:	43614.100				
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:	11257700
Application Number:	95001792
International Application Number:	
Confirmation Number:	1972
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180 .
Customer Number:	27683
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.100
Receipt Date:	25-OCT-2011
Filing Date:	
Time Stamp:	11:57:39
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$8800
RAM confirmation Number	10516
Deposit Account	081394
Authorized User	MCCOMBS,DAVID L

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	Transmittal of New Application	Transmittal_Request_For_Inter_Partes_Reexamination.pdf	83893 eedc387e66d329d42b3e4d0235e5796fb12c275	no	3
Warnings:					
Information:					
2	Reexam - Info Disclosure Statement Filed by 3rd Party	Modified_PTO_Form_1449.pdf	35241 c43f3e5b5ebc79a26ccaa2e35325e5b966fb74f	no	1
Warnings:					
Information:					
3		Inter_Partes_Request_For_Reexamination_of_Patent.pdf	1398056 e7d435db1720b47ed43785587d411cddfca bcb1	yes	28
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Receipt of Original Inter Partes Reexam Request	1	27	
		Reexam Certificate of Service	28	28	
Warnings:					
Information:					
4	Copy of patent for which reexamination is requested	Ex_A_pat7188180.pdf	5232014 4e7d238f27408026996276328d9327292b9e1809	no	84
Warnings:					
Information:					
5	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B1P1_FH_7188180.pdf	8443201 ac51e27cf2cb58162165ca81523d9cd5b9471936	no	200
Warnings:					
Information:					
6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B1P2_FH_7188180.pdf	7011442 fa94b4b7706055d46b27c24d94e37b0151f187c3	no	162
Warnings:					
Information:					
7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B2P1_FH_App_09558209.pdf	9684658 a662caec15082028dd6a80ce55fec6173be7059e	no	201
Warnings:					
Information:					

8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B2P2_FH_App_09558209.pdf	11401120 9c749743727c7aeda566c379d74b2b7ef59a672	no	201
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B2P3_FH_App_09558209.pdf	12849255 0df90117d3f7332c1fddcd0e9f0a17c3365b7eb2	no	220
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B3P1_FH_95001270.pdf	10369292 36a8283a922ba4c3d02aafd20d03eb13f01e187	no	200
Warnings:					
Information:					
11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B3P2_FH_95001270.pdf	10711934 cf4156cef5ee7e0fe60ad8e676bcc1ffb0eae077	no	200
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B3P3_FH_95001270.pdf	7084933 fd50d4fbb2962a3c5144bc8675b05f4000606889	no	200
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B3P4_FH_95001270.pdf	10628064 9fe44efc6efb07db2712ab6eac92f1911499de8	no	200
Warnings:					
Information:					
14	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B3P5_FH_95001270.pdf	9825921 60afd55f58c6a1488f1a568b3468dbc35829795	no	204
Warnings:					
Information:					
15	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_B4_VirnetX_v_Microsoft_Markman_Order.pdf	782732 3245e637bfd790c75ce23574c595d5eccc98fc3	no	36
Warnings:					
Information:					
16	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_C1_US6502135.pdf	4566191 63b918639381382a348e07decafd247555abb390	no	73
Warnings:					
Information:					

17	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_C2_US7010604.pdf	2728560	no	45
			020713d2eb1e3e7505098b7f795cf9de7be1abe		
Warnings:					
Information:					
18	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_C3_Prov_60106261.pdf	1998596	no	43
			e77dc27d834a90176866a57d58cabf85734c27bf		
Warnings:					
Information:					
19	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_C4_Prov_60137704.pdf	1508366	no	30
			58517000021b782a8d123111188114542cd4d371		
Warnings:					
Information:					
20	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D1P1_Lendenmann.pdf	5376240	no	200
			7b463aeadd665ce8c5cc57f49d8e7d286eb34f03		
Warnings:					
Information:					
21	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D1P2_Lendenmann.pdf	1153970	no	76
			57a46593a65b7e977d65fba1e35a640d65dfbaa4		
Warnings:					
Information:					
22	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D2_Kiuchi.pdf	959556	no	13
			7f2f8e27b26509fb12e4e7f3079f879175911a1		
Warnings:					
Information:					
23	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D3_Solana.pdf	740735	no	16
			198581f36e8718198b85256c63a1aac467d5377a		
Warnings:					
Information:					
24	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D4_Martin.pdf	2216520	no	15
			ef6c90337512d464312e23da0955c84fc5e8eb3a		
Warnings:					
Information:					
25	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D5P1_Schneier.pdf	11458771	no	200
			b3095bd03d9d94fab31c7a4fb5450be2415b6533		
Warnings:					
Information:					

26	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D5P2_Schneier.pdf	9909066 ffab84e78446b9e5ac5b8f50fb8829f100c9757	no	200
Warnings:					
Information:					
27	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D5P3_Schneier.pdf	9437936 5f5f24bdcae9c8c8dd225771500c75cef59b2a9b	no	200
Warnings:					
Information:					
28	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D5P4_Schneier.pdf	10249981 93e708d05f2061dd8770891cf6be0f8461ae2fa7	no	190
Warnings:					
Information:					
29	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D6_rfc793.pdf	904843 db0de4853ec79fd8b3536ae81fd9a686a572ca8ca	no	90
Warnings:					
Information:					
30	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D7_Schimpf_Securing_Web_Access.pdf	3155839 354d8be461d28cbafc89bae9acc86c307c211fbc	no	8
Warnings:					
Information:					
31	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D8P1_Rosenberry_Understanding_DCE.pdf	11710205 a709e6bbce4cfb47d96c80b9f149e7cb737fb75b	no	200
Warnings:					
Information:					
32	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D8P2_Rosenberry_Understanding_DCE.pdf	3056769 2e346a75a34b29a417d1ea9f340ee900be079f43	no	75
Warnings:					
Information:					
33	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D9_Masys_Nov_11_1998.pdf	876483 a715e0933a47c2f6441e7744e5cc32d32a7b3f93	no	6
Warnings:					
Information:					
34	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_D10_RFC1034.pdf	288502 ac1f7d2d5e7b451103961fcc4c3625e6c5d7e62a	no	57
Warnings:					
Information:					

35	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_E1_Lendenmann.pdf	2715934	no	79
			71152bede248854aa24cf446dff9a9d8c0805eb		
Warnings:					
Information:					
36	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_E2_Kiuchi.pdf	1736999	no	53
			45bc450d6018a9755f21b2140e9d0dcb5e4df059		
Warnings:					
Information:					
37	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_E3_Solana.pdf	435378	no	18
			0ef906f4dc944765d715264bfc5158e6a671774		
Warnings:					
Information:					
38	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_E4_Schimpf.pdf	632868	no	20
			d580b3b15d900493024aaa59707310c0344dd86e		
Warnings:					
Information:					
39	Fee Worksheet (SB06)	fee-info.pdf	30164	no	2
			2a89f00f0cb2a72d8ba3264be8830889938c8709		
Warnings:					
Information:					
Total Files Size (in bytes):			193390228		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					