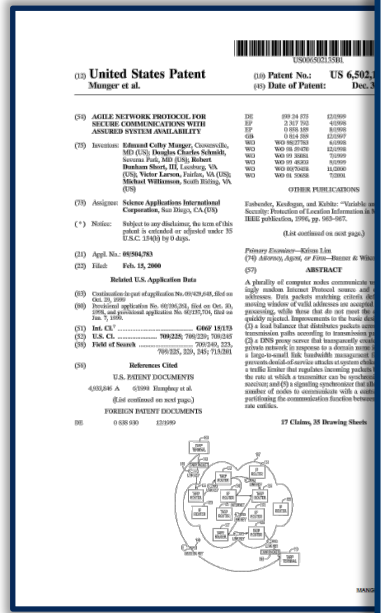
IPR2015-01046, -01047

135 Patent

135 Patent
Ex. 1001



US006502135B1

(12) United States Patent
Munger et al.

(10) Patent No.: US 6,502,1

(45) Date of Patent: Dec. 3

(54) AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

(75) Inventors: Edmund Colby Munger, Crownsville, MD (US); Douglas Charles Schmidt, Severna Park, MD (US); Robert Dunham Short, III, Leesburg, VA (US); Victor Larson, Fairfax, VA (US); Michael Williamson, South Riding, VA (US)

(73) Assignee: Science Applications International Corporation, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/504,783

(22) Filed: Feb. 15, 2000

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) Int. Cl.^{7} G06F 15/173

(52) U.S. Cl. 709/225; 709/229; 709/245

(58) Field of Search 709/249, 223, 709/225, 229, 245; 713/201

(56) References Cited

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable an Security: Protection of Location Information in M IEEE publication, 1996, pp. 963–967.

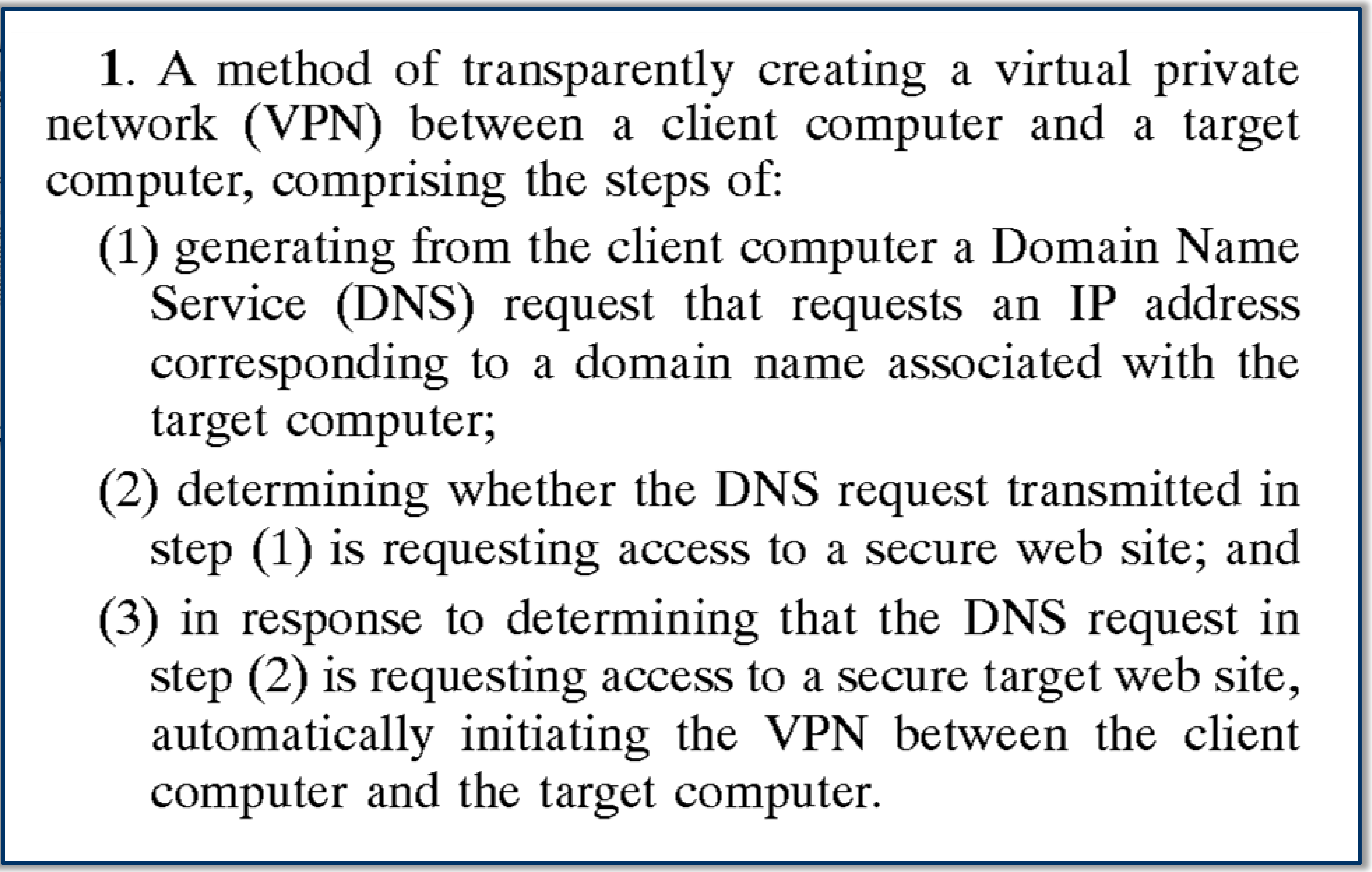
(List continued on next page.)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witc

(57) ABSTRACT

A plurality of computer nodes communicate us ingly random Internet Protocol source and d addresses. Data packets matching criteria def moving window of valid addresses are accepted processing, while those that do not meet the quickly rejected. Improvements to the basic desi (1) a load balancer that distributes packets acros transmission paths according to transmission pa (2) a DNS proxy server that transparently creat private network in response to a domain name i a large-to-small link bandwidth management f prevents denial-of-service attacks at system choke a traffic limiter that regulates incoming packets b the rate at which a transmitter can be synchroni receiver; and (5) a signaling synchronizer that all number of nodes to communicate with a centr partitioning the communication function betwee rate entities.

17 Claims, 35 Drawing Sheets



1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

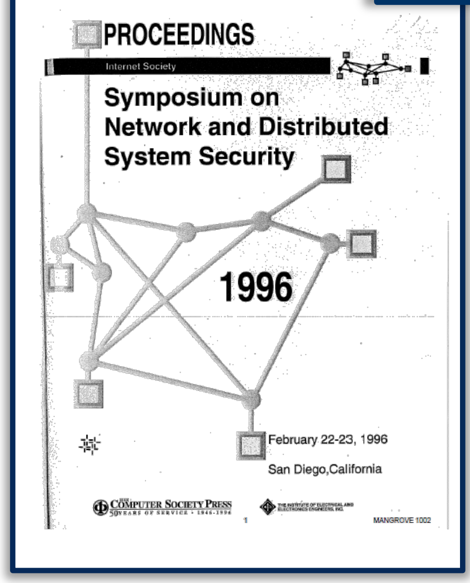
(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

Kiuchi

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

Symposium on Network and Distributed System Security

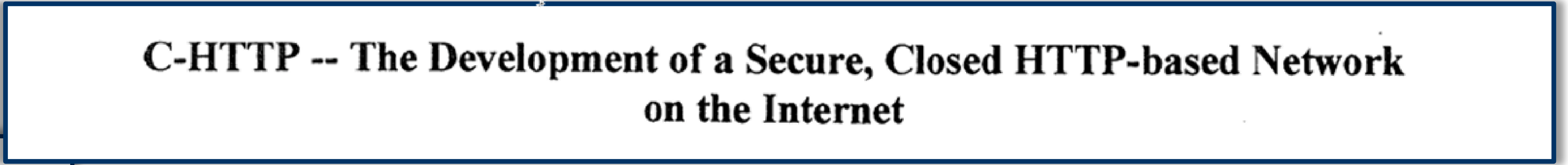
1996

February 22-23, 1996

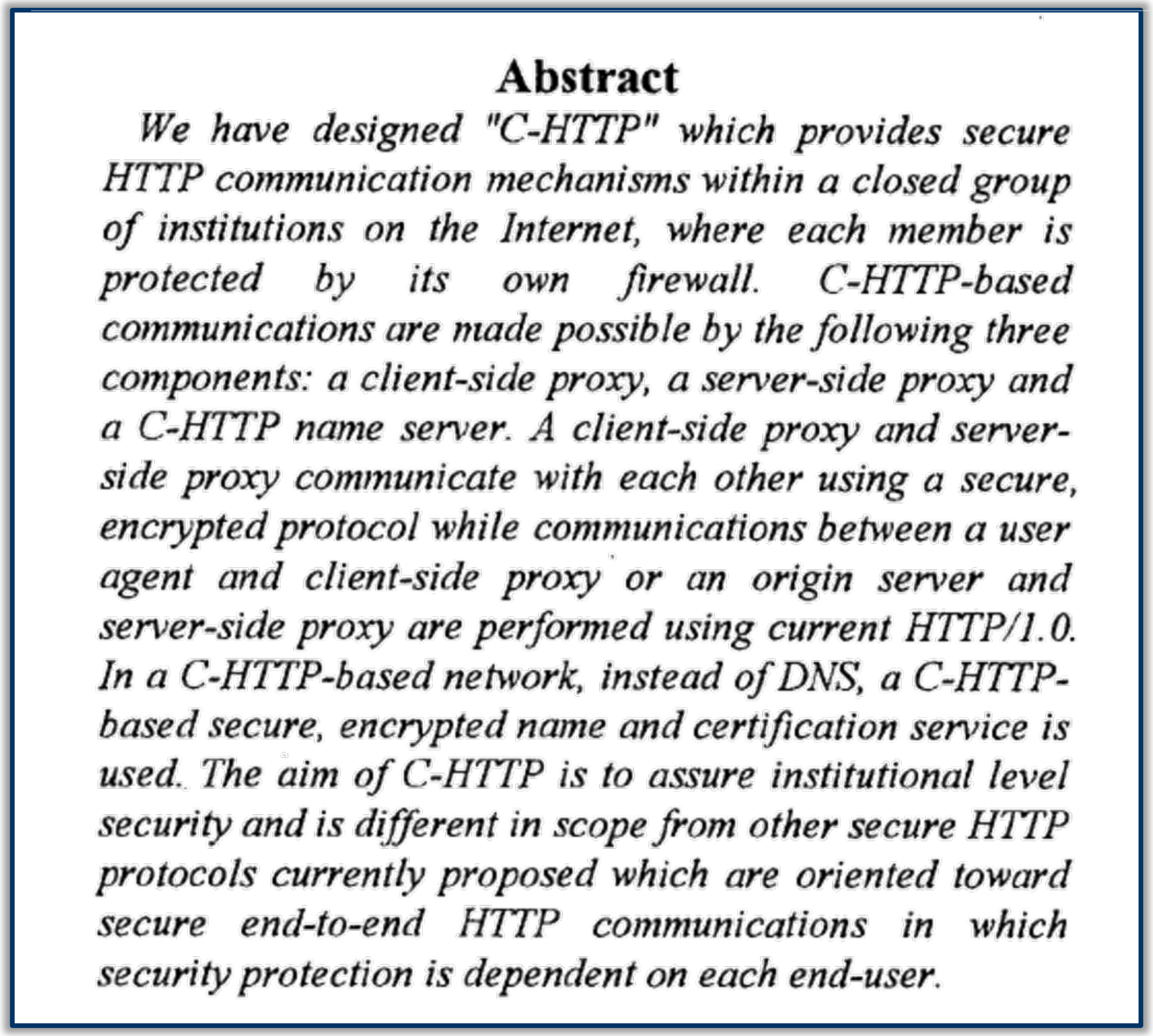
San Diego,California

COMPUTER SOCIETY PRESS

MANGROVE 1002



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



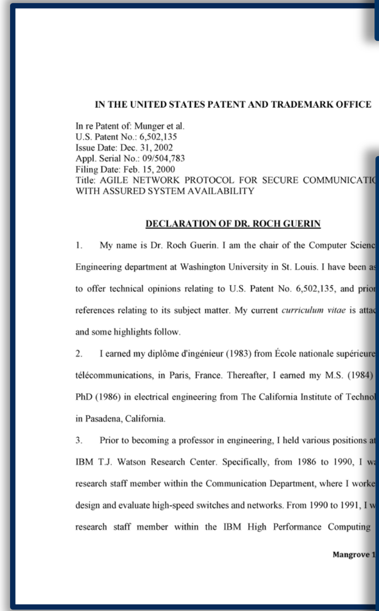
Abstract

We have designed "C-HTTP" which provides secure HTTP communication mechanisms within a closed group of institutions on the Internet, where each member is protected by its own firewall. C-HTTP-based communications are made possible by the following three components: a client-side proxy, a server-side proxy and a C-HTTP name server. A 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 current HTTP/1.0. In a C-HTTP-based network, instead of DNS, a C-HTTP-based secure, encrypted name and certification service is used. The aim of C-HTTP is to assure institutional level security and is different in scope from other secure HTTP protocols currently proposed which are oriented toward secure end-to-end HTTP communications in which security protection is dependent on each end-user.

Kiuchi at 64
135 Pet. at 18-19, 26
151 Pet. at 17-18

Kiuchi

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIC
WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUERIN

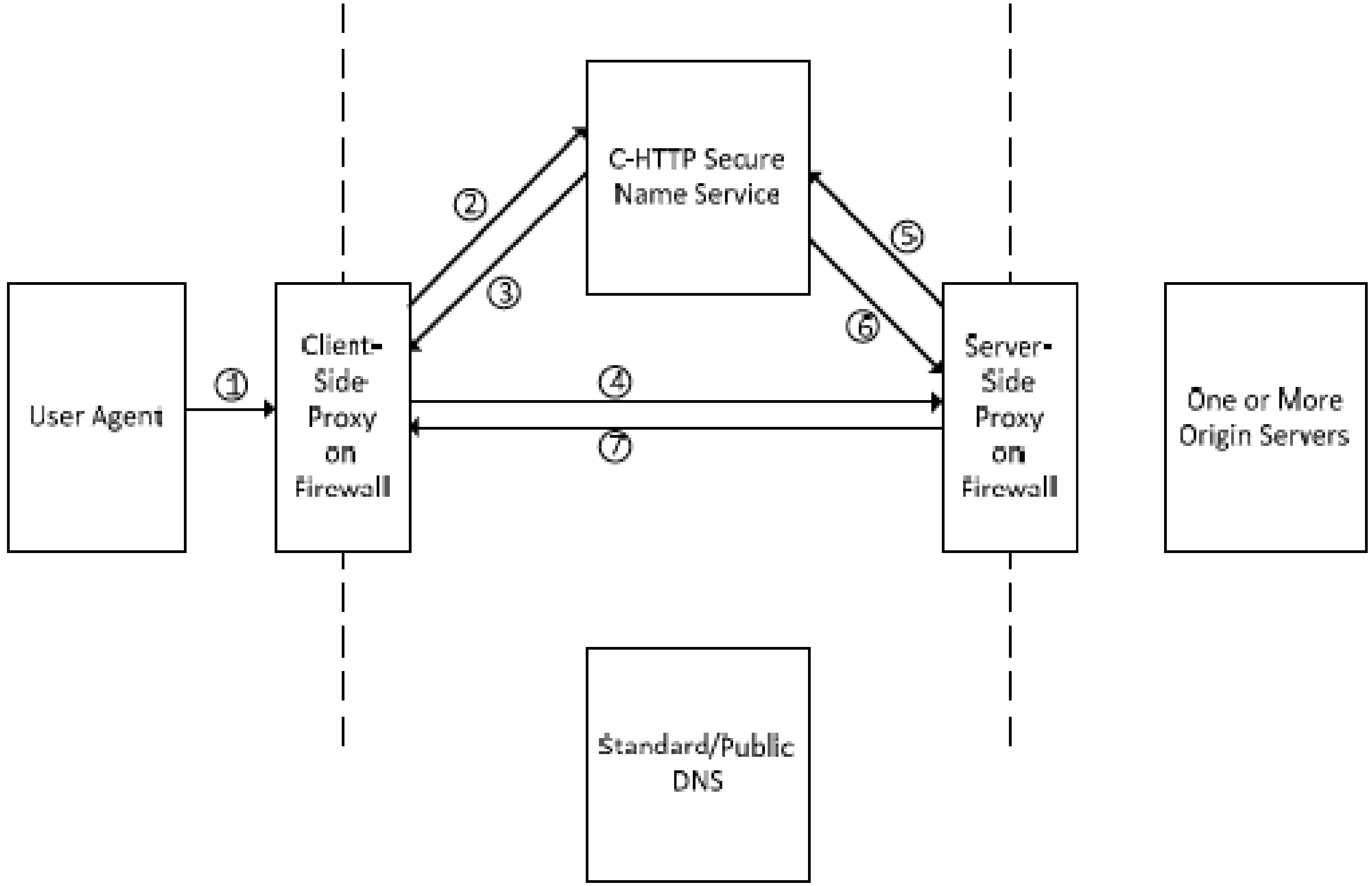
1. My name is Dr. Roch Guerin. I am the chair of the Computer Scienc
Engineering department at Washington University in St. Louis. I have been as
to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior
references relating to its subject matter. My current *curriculum vitae* is attac
and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure
télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984)
PhD (1986) in electrical engineering from The California Institute of Technol
in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at
IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I wa
research staff member within the Communication Department, where I worke
design and evaluate high-speed switches and networks. From 1990 to 1991, I w
research staff member within the IBM High Performance Computing

Mangrove 1

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



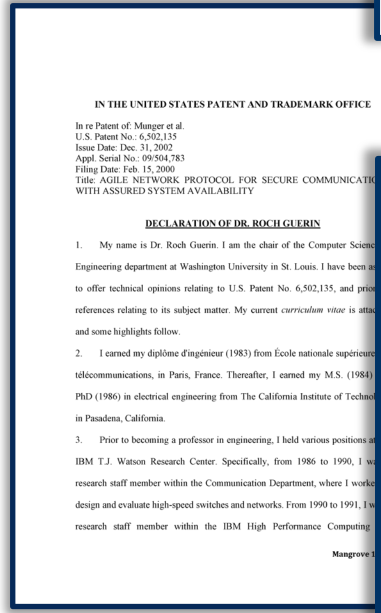
C-HTTP Secure Name Service
②
③
⑤
⑥
User Agent
①
Client-Side Proxy on Firewall
④
⑦
Server-Side Proxy on Firewall
One or More Origin Servers
Standard/Public DNS

Diagram 2

135 Pet. (Paper 5) at 20; Ex. 1003 at ¶21
151 Pet. (Paper 5) at 19; Ex. 1003 at ¶19

Kiuchi

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIO
WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Scienc Engineering department at Washington University in St. Louis. I have been as to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior references relating to its subject matter. My current *curriculum vitae* is attac and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) PhD (1986) in electrical engineering from The California Institute of Technol in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I wa research staff member within the Communication Department, where I worke design and evaluate high-speed switches and networks. From 1990 to 1991, I w research staff member within the IBM High Performance Computing

Mangrove 1

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

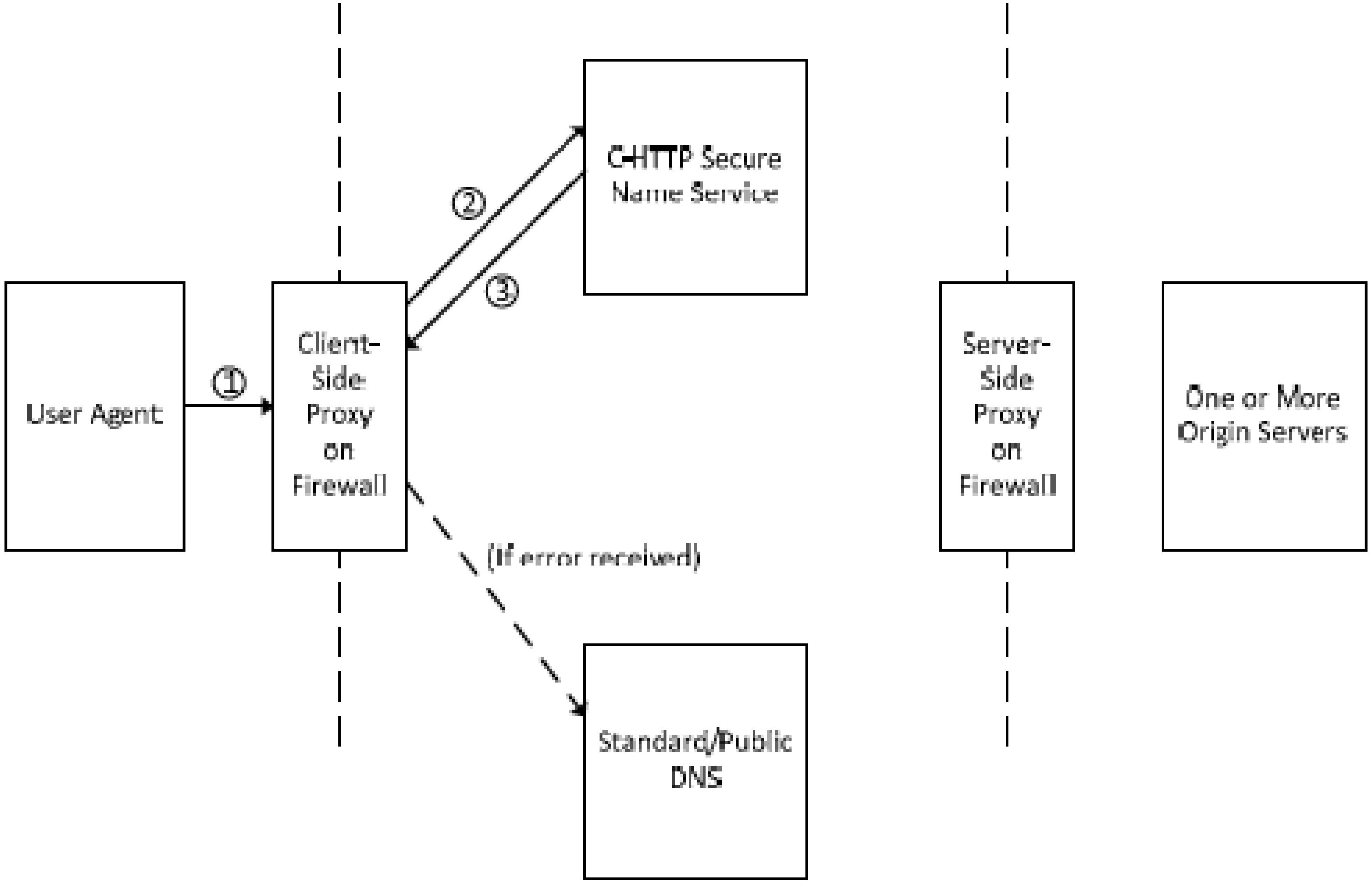
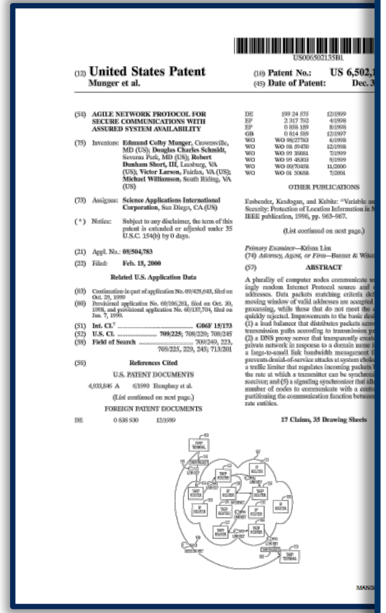

C-HTTP Secure Name Service
②
③
User Agent
①
Client-Side Proxy on Firewall
Server-Side Proxy on Firewall
One or More Origin Servers
(If error received)
Standard/Public DNS

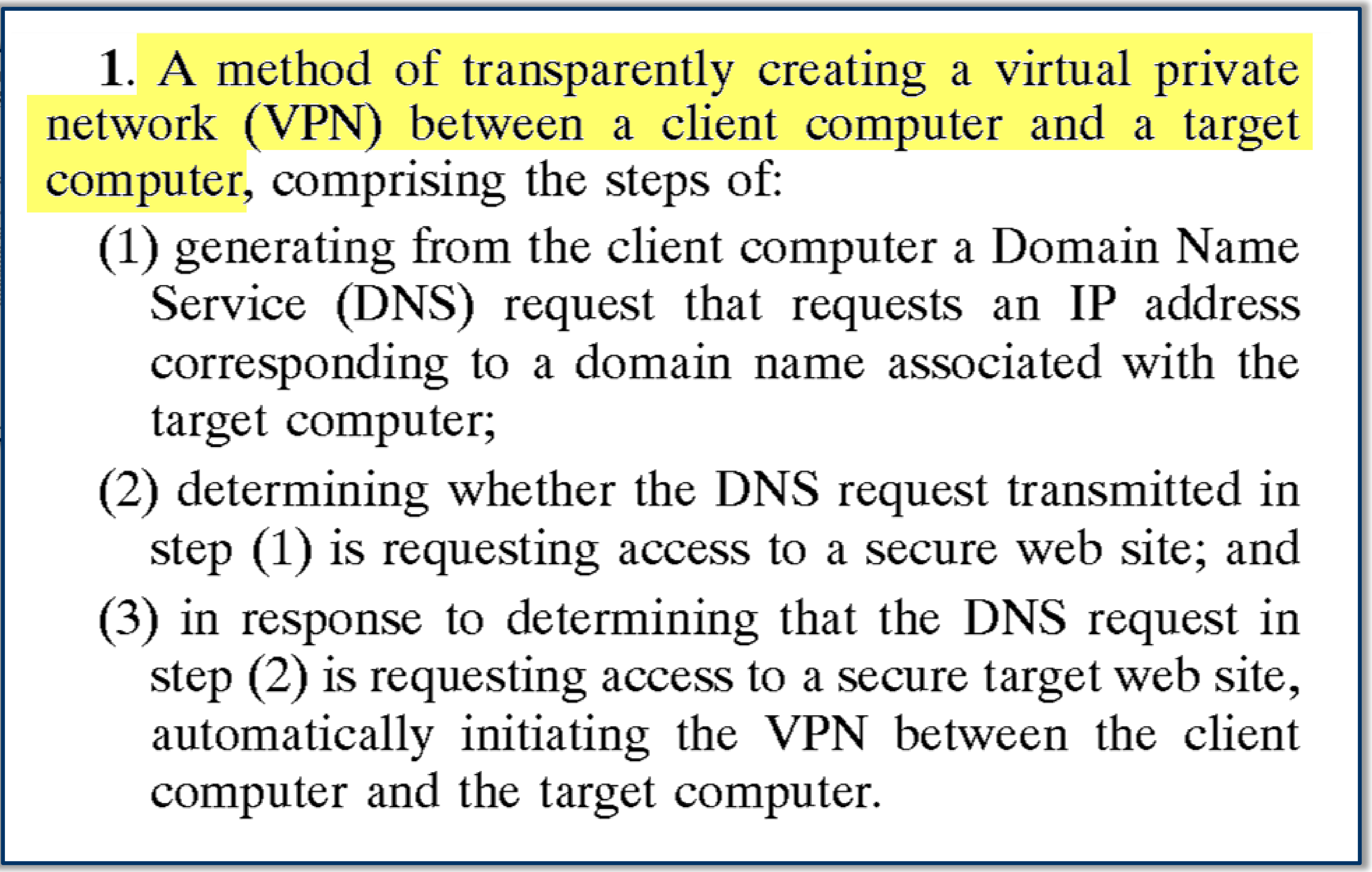
Diagram 3

135 Pet. (Paper 5) at 21; Ex. 1003 at ¶25
151 Pet. (Paper 5) at 20; Ex. 1003 at ¶24

135 Patent: Preamble

135 Patent
Ex. 1001





1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

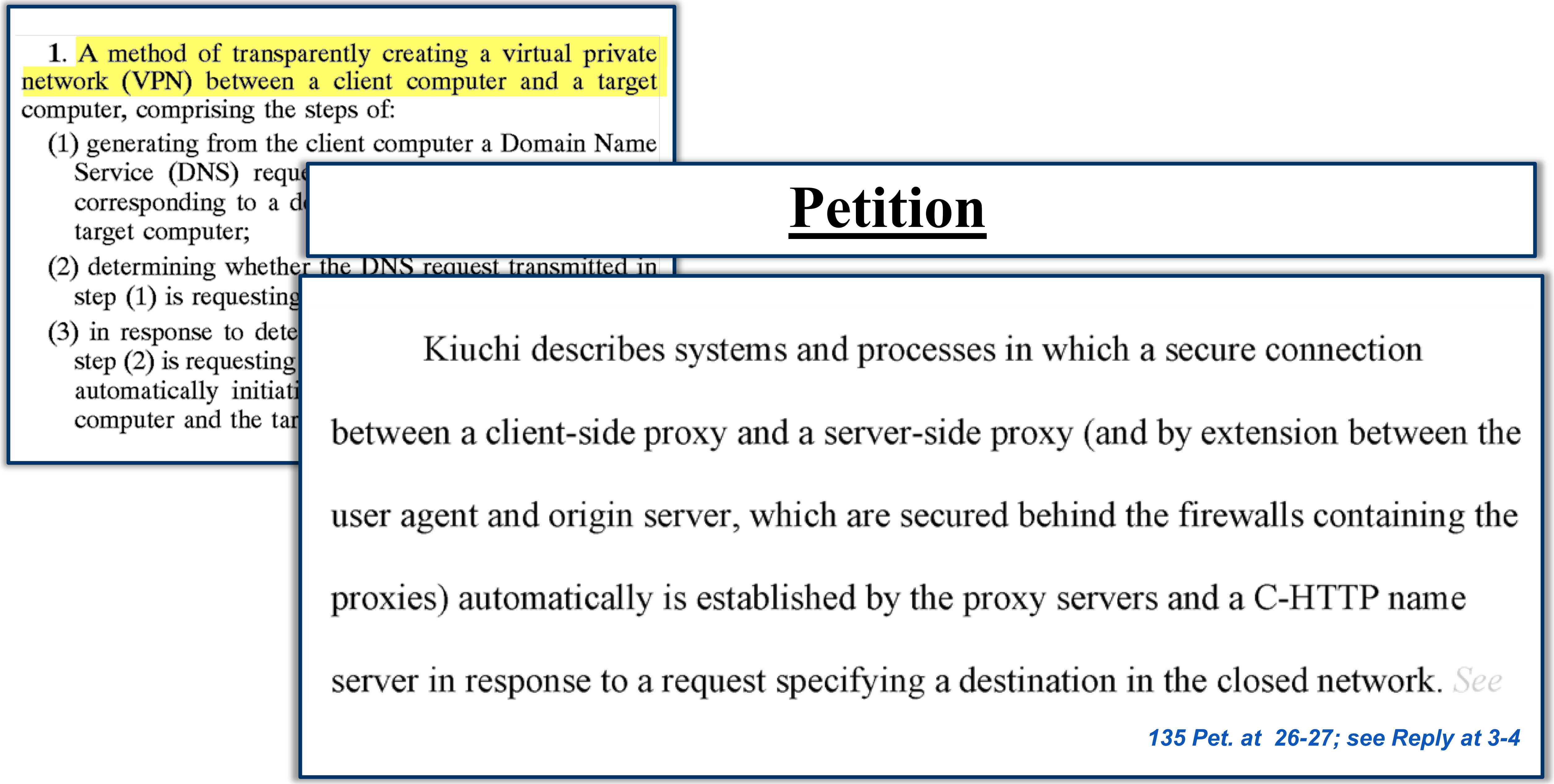
(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

135 Claim 1: Preamble

135 Patent Claim 1



1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) reque
corresponding to a d
target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting

(3) in response to dete
step (2) is requesting
automatically initiati
computer and the tar

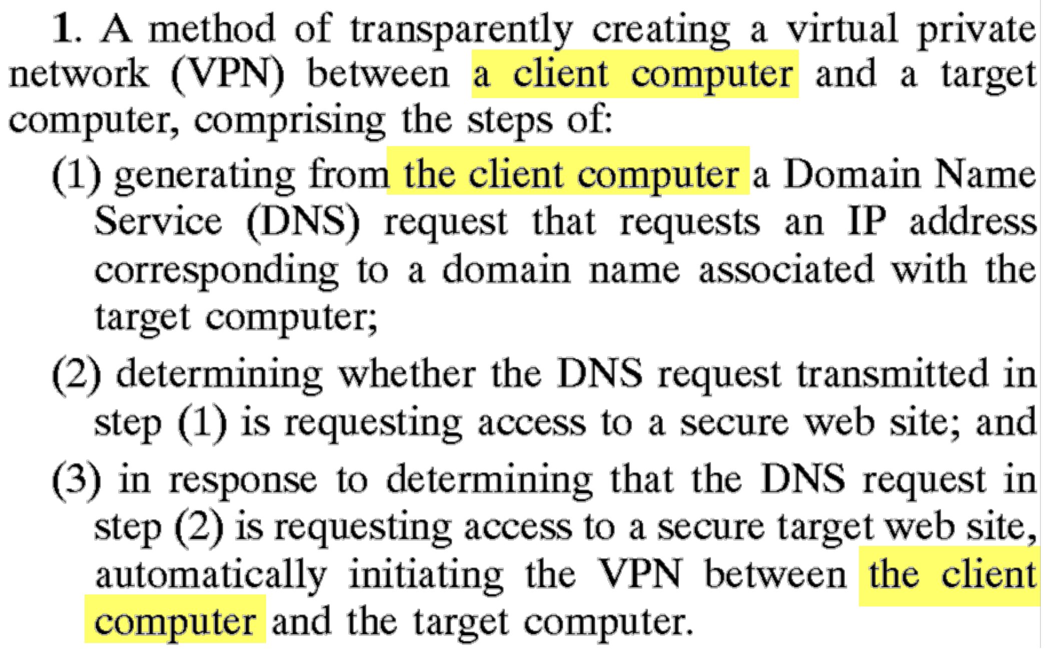
Petition

Kiuchi describes systems and processes in which a secure connection between a client-side proxy and a server-side proxy (and by extension between the user agent and origin server, which are secured behind the firewalls containing the proxies) automatically is established by the proxy servers and a C-HTTP name server in response to a request specifying a destination in the closed network. *See*

135 Pet. at 26-27; see Reply at 3-4

135 Patent: Client Computer

135 Patent Claim 1



1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

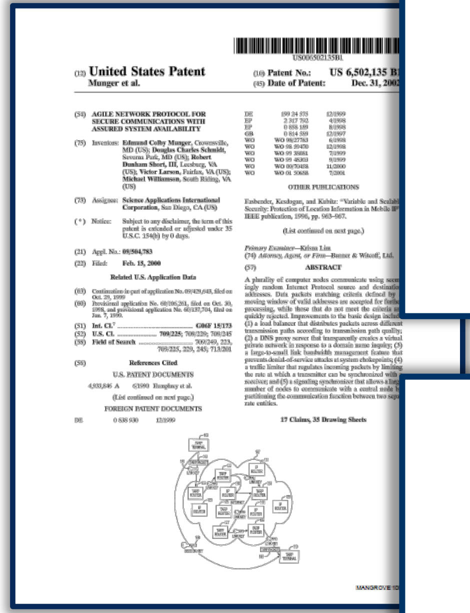
Client Computer

Petitioners' Construction	Patent Owner's Construction
A computer from which a data request to a server is generated	User's Computer

135 Petition at 15-16; Resp. at 15

The Patent Describes a “Conventional Client”

135 Patent
Ex. 1001



US006502135B1

(12) **United States Patent**
Munger et al.

(10) **Patent No.:** **US 6,502,135 B**
(45) **Date of Patent:** **Dec. 31, 2002**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY**

(75) Inventors: **Edmund Colby Munger**, Crownsville, MD (US); **Douglas Charles Schmidt**, Severna Park, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Science Applications International Corporation**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/504,783**

(22) Filed: **Feb. 15, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**7 .... **G06F 15/173**
(52) **U.S. Cl.** **709/225**; 709/229; 709/245
(58) **Field of Search** 709/249, 223, 709/225, 229, 245; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Eschenauer, Kesdogan, and Kubitz: “Variable and Scalabl Security: Protection of Location Information in Mobile IP” IEEE publication, 1996, pp. 963–967.

(List continued on next page.)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destinatio addresses. Data packets matching criteria defined by moving window of valid addresses are accepted for furthe processing, while those that do not meet the criteria ar quickly rejected. Improvements to the basic design includ (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 receiver; and (5) a signaling synchronizer that allows a larg number of nodes to communicate with a central node b partitioning the communication function between two sepa rate entities.

17 Claims, 35 Drawing Sheets

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

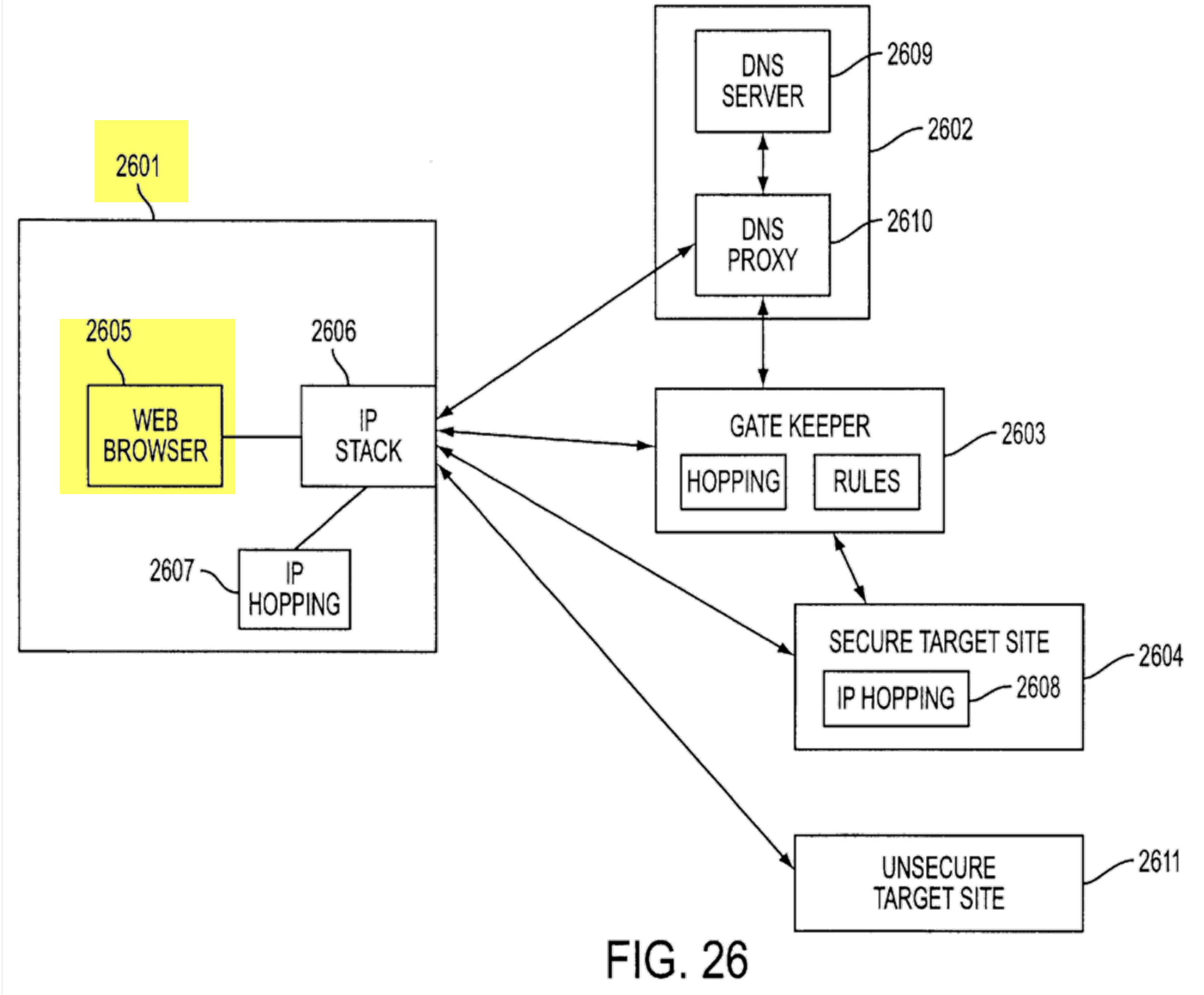
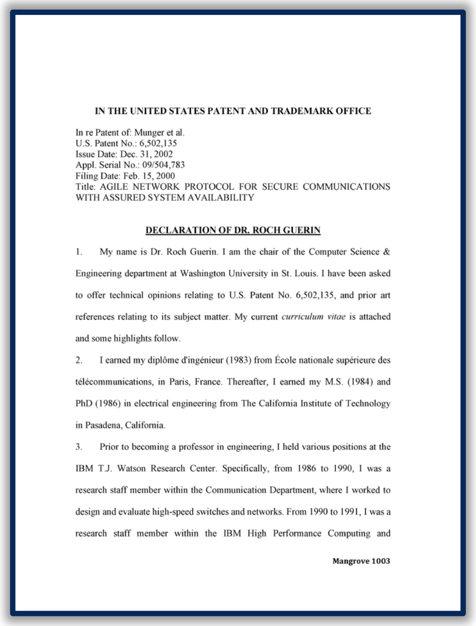


FIG. 26

135 Patent at Fig. 26, 38:13-17;
Reply at 9

Dr. Guerin: A “Client” Makes Requests

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Science & Engineering department at Washington University in St. Louis. I have been asked to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior art references relating to its subject matter. My current *curriculum vitae* is attached and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure des télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) and PhD (1986) in electrical engineering from The California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at the IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I was a research staff member within the Communication Department, where I worked to design and evaluate high-speed switches and networks. From 1990 to 1991, I was a research staff member within the IBM High Performance Computing and

Mangrove 1003

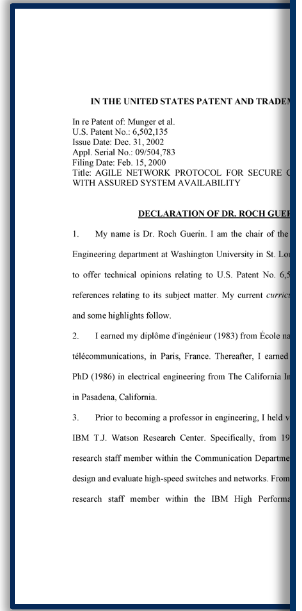
Dr. Guerin

origin server associated with the server-side proxy. *See* Ex. 1002, p. 64, § 2.1. In particular, the client-side proxy performs various steps on behalf of the user agent to facilitate communications with an origin server and provides responses to a user agent’s resource requests. The C-HTTP connection established by the client-side proxy of Kiuchi relies on HTTP 1.0 exchanges as would any regular HTTP communication, and therefore the client-side proxy acts as a client computer in its communication with the server-side proxy and as a server in its communication with the user agent. *See* Ex. 1002, p. 67, § 4.2; *see also* Ex. 1014, p. 5 (T. Berners-Lee et al., *Hypertext Transfer Protocol -- HTTP/1.0*, RFC 1945, May 1996)) (describing proxy as an “intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients”).

Ex. 1003 at ¶19; Pet. at 19, 26-27; Reply at 10

Dr. Guerin: A “Client” Makes Requests

Dr. Gue
Ex. 10



IN THE UNITED STATES PATENT AND TRADE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE C
WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUE

1. My name is Dr. Roch Guerin. I am the chair of the Engineering department at Washington University in St. Lo to offer technical opinions relating to U.S. Patent No. 6,5 references relating to its subject matter. My current *curric* and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École na télécommunications, in Paris, France. Thereafter, I earned PhD (1986) in electrical engineering from The California In in Pasadena, California.

3. Prior to becoming a professor in engineering, I held v IBM T.J. Watson Research Center. Specifically, from 19 research staff member within the Communication Departme design and evaluate high-speed switches and networks. From research staff member within the IBM High Performa

RFC 1945

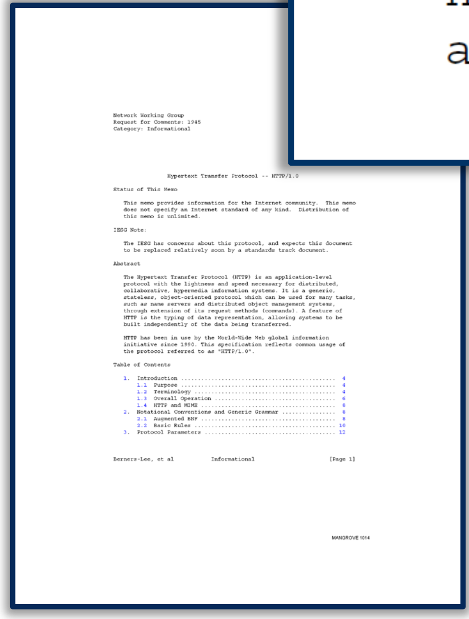
```
client

   An application program that establishes connections for the
   purpose of sending requests.

proxy

   An intermediary program which acts as both a server and a client
   for the purpose of making requests on behalf of other clients.
   Requests are serviced internally or by passing them, with
   possible translation, on to other servers. A proxy must
   interpret and, if necessary, rewrite a request message before
   forwarding it. Proxies are often used as client-side portals
   through network firewalls and as helper applications for
   handling requests via protocols not implemented by the user
   agent.
```

Ex. 1014 at 5-6; Pet. at 26-27 (citing Ex. 1003 ¶19); Reply at 10

1. In
agent
a user
t-side
HTTP
in its
cation

with the user agent. *See* Ex. 1002, p. 67, § 4.2; *see also* Ex. 1014, p. 5 (T. Berners-Lee et al., *Hypertext Transfer Protocol -- HTTP/1.0*, RFC 1945, May 1996)) (describing proxy as an “intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients”).

Ex. 1003 at ¶19; Pet. at 19, 26-27; Reply at 10



```
Network Working Group
Request for Comments: 1945
Category: Informational


                 Hypertext Transfer Protocol -- HTTP/1.0

Status of This Memo

   This memo provides information for the Internet community.  This memo
   does not specify an Internet standard of any kind.  Distribution of
   this memo is unlimited.

IESG Note:

   The IESG has concerns about this protocol, and expects this document
   to be replaced relatively soon by a standards track document.

Abstract

   The Hypertext Transfer Protocol (HTTP) is an application-level
   protocol with the lightness and speed necessary for distributed,
   collaborative, hypermedia information systems. It is a generic,
   stateless, object-oriented protocol which can be used for many tasks,
   such as name servers and distributed object management systems,
   through extension of its request methods (commands). A feature of
   HTTP is the typing of data representation, allowing systems to be
   built independently of the data being transferred.

   HTTP has been in use by the World-Wide Web global information
   initiative since 1990. This specification reflects common usage of
   the protocol referred to as "HTTP/1.0".

Table of Contents

   1.  Introduction ............................................  4
       1.1  Purpose ............................................  4
       1.2  Terminology ........................................  4
       1.3  Overall Operation ..................................  6
       1.4  HTTP and MIME ......................................  8
   2.  Notational Conventions and Generic Grammar ..............  8
       2.1  Augmented BNF ......................................  8
       2.2  Basic Rules ........................................ 10
   3.  Protocol Parameters ..................................... 12


Berners-Lee, et al          Informational                     [Page 1]
```

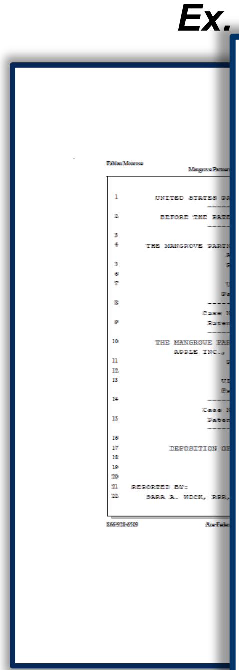
MANGROVE 1014

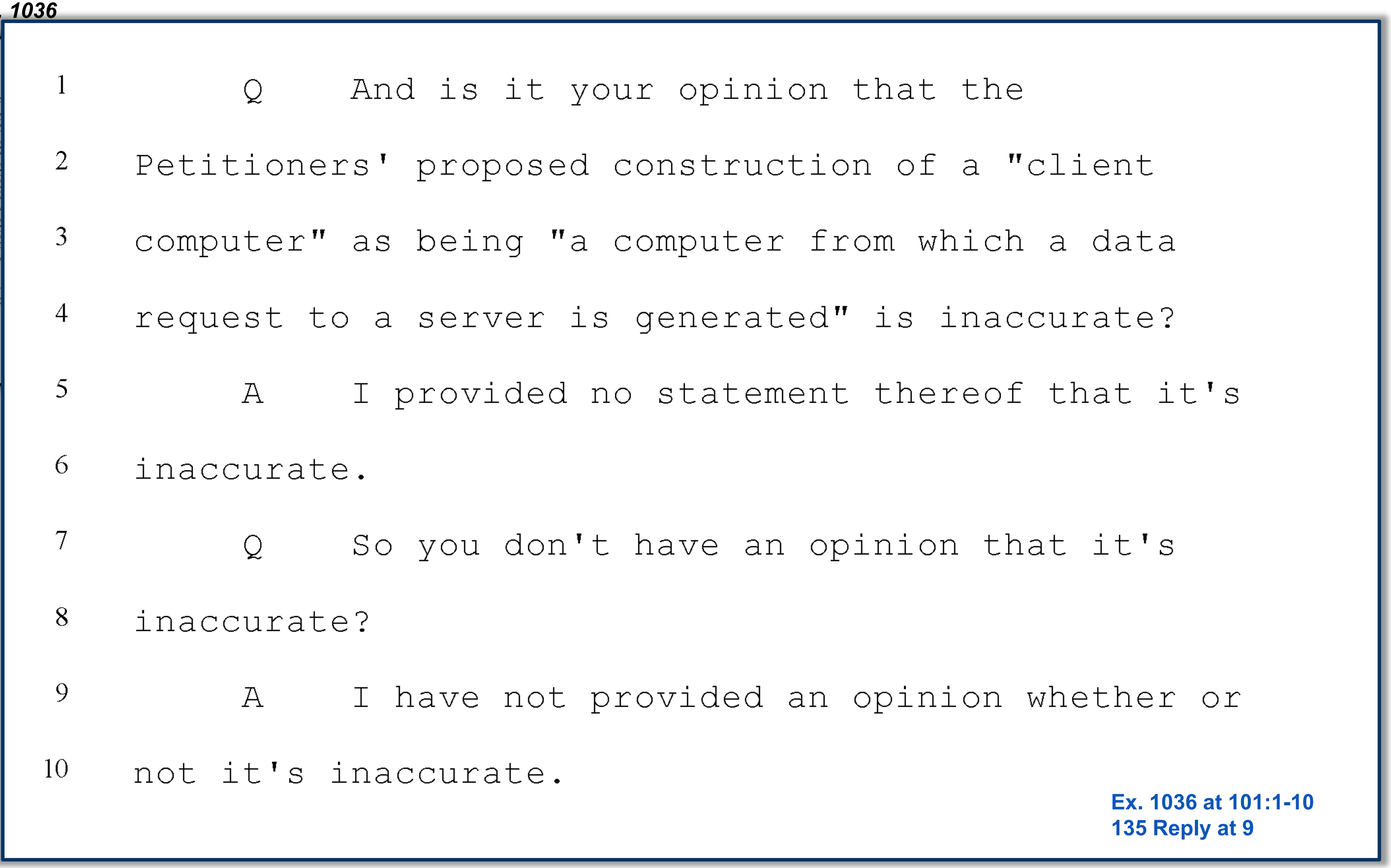
RFC 1945
Ex. 1014

Dr. Monrose: Petitioners’ Construction of Client Computer

Ex. 1036 – Deposition Transcript of Dr. Fabian Monrose (April 28, 2016)

Monrose Dep. Ex. 1036





Q And is it your opinion that the Petitioners' proposed construction of a "client computer" as being "a computer from which a data request to a server is generated" is inaccurate?

A I provided no statement thereof that it's inaccurate.

Q So you don't have an opinion that it's inaccurate?

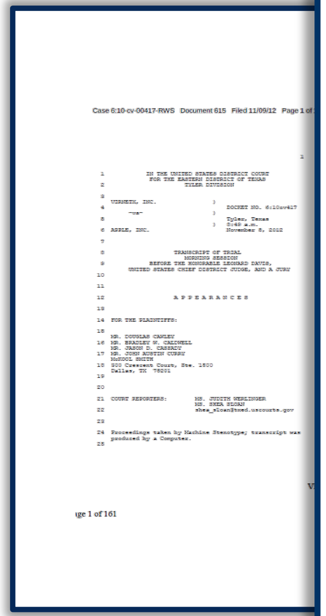
A I have not provided an opinion whether or not it's inaccurate.

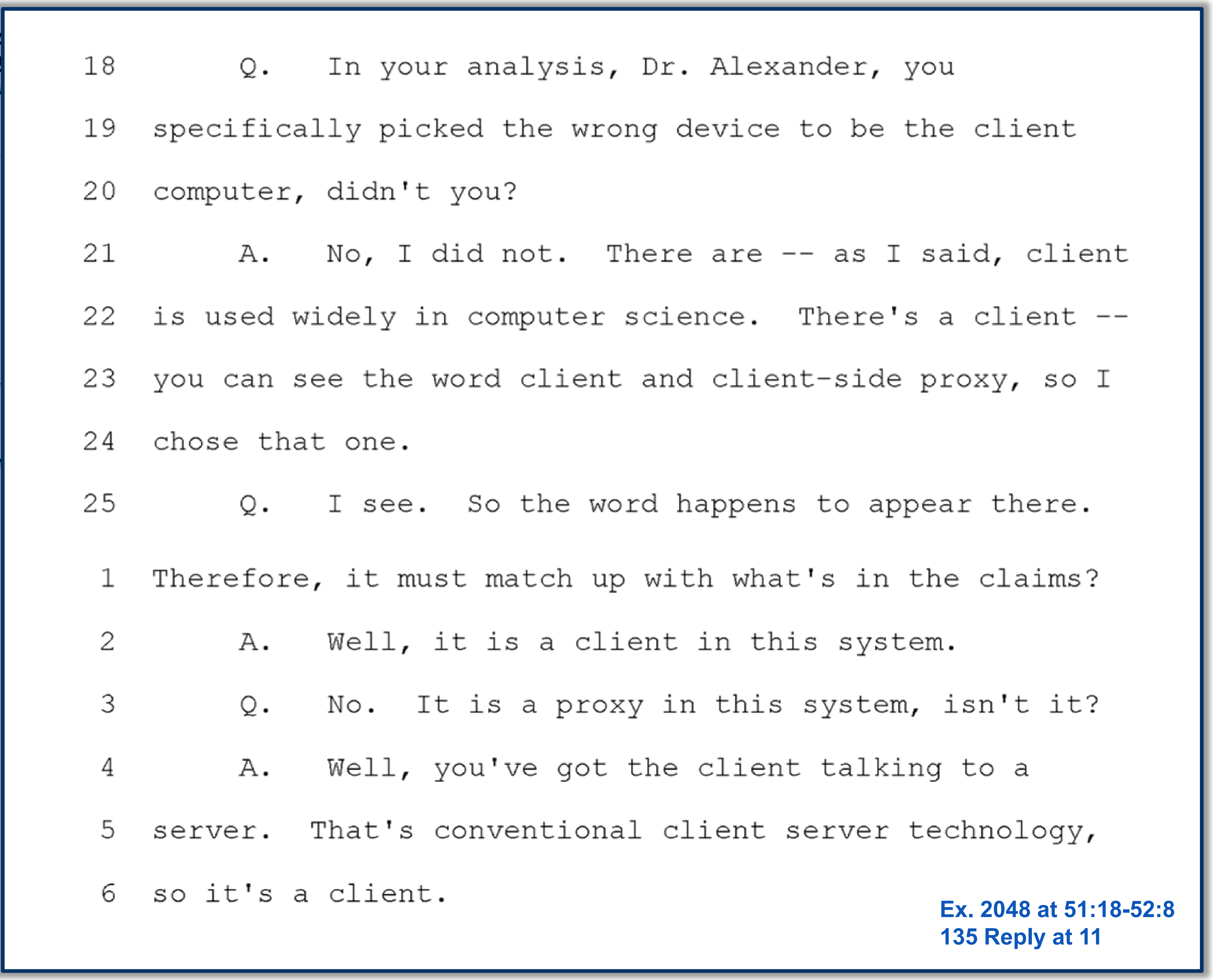
Ex. 1036 at 101:1-10
135 Reply at 9

Apple's Position In District Court: Client Computer

Ex. 2048 – Transcript of Trial, Morning Session (E.D. Tex. Nov. 5, 2012)

Trial Transc
Ex. 204





Q. In your analysis, Dr. Alexander, you specifically picked the wrong device to be the client computer, didn't you?

A. No, I did not. There are -- as I said, client is used widely in computer science. There's a client -- you can see the word client and client-side proxy, so I chose that one.

Q. I see. So the word happens to appear there. Therefore, it must match up with what's in the claims?

A. Well, it is a client in this system.

Q. No. It is a proxy in this system, isn't it?

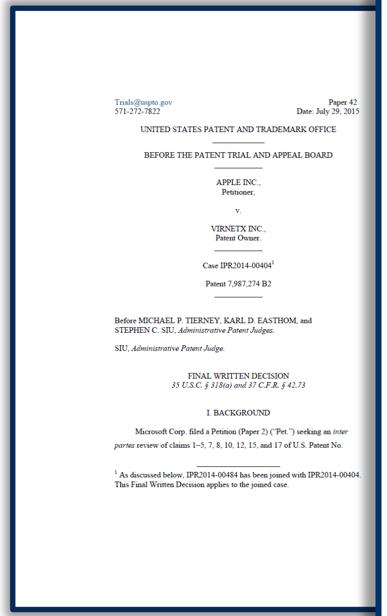
A. Well, you've got the client talking to a server. That's conventional client server technology, so it's a client.

Ex. 2048 at 51:18-52:8
135 Reply at 11

IPR2014-00404: “Client” Computer”

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404 Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

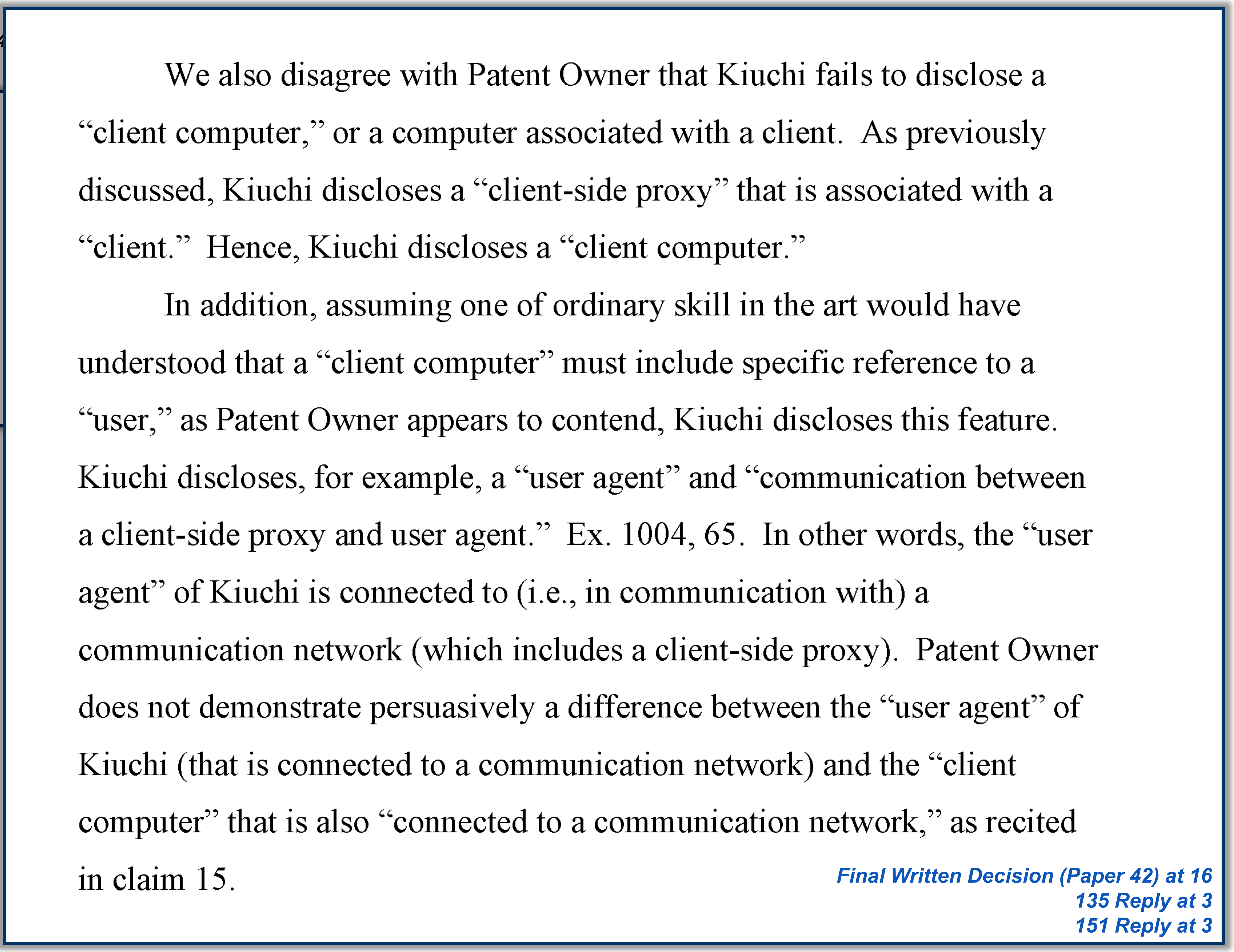
SIU, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Microsoft Corp. filed a Petition (Paper 2) (“Pet.”) seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

[1] As discussed below, IPR2014-00484 has been joined with IPR2014-00404. This Final Written Decision applies to the joined case.



We also disagree with Patent Owner that Kiuchi fails to disclose a “client computer,” or a computer associated with a client. As previously discussed, Kiuchi discloses a “client-side proxy” that is associated with a “client.” Hence, Kiuchi discloses a “client computer.”

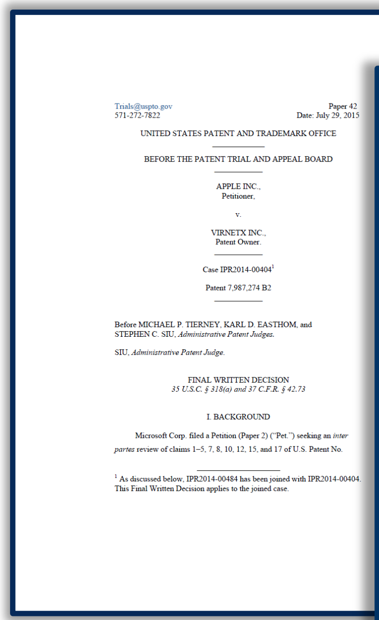
In addition, assuming one of ordinary skill in the art would have understood that a “client computer” must include specific reference to a “user,” as Patent Owner appears to contend, Kiuchi discloses this feature. Kiuchi discloses, for example, a “user agent” and “communication between a client-side proxy and user agent.” Ex. 1004, 65. In other words, the “user agent” of Kiuchi is connected to (i.e., in communication with) a communication network (which includes a client-side proxy). Patent Owner does not demonstrate persuasively a difference between the “user agent” of Kiuchi (that is connected to a communication network) and the “client computer” that is also “connected to a communication network,” as recited in claim 15.

Final Written Decision (Paper 42) at 16
135 Reply at 3
151 Reply at 3

IPR2014-00404: “Client” Computer”

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404
Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

SIU, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Microsoft Corp. filed a Petition (Paper 2) (“Pet.”) seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

[1] As discussed below, IPR2014-00484 has been joined with IPR2014-00404. This Final Written Decision applies to the joined case.

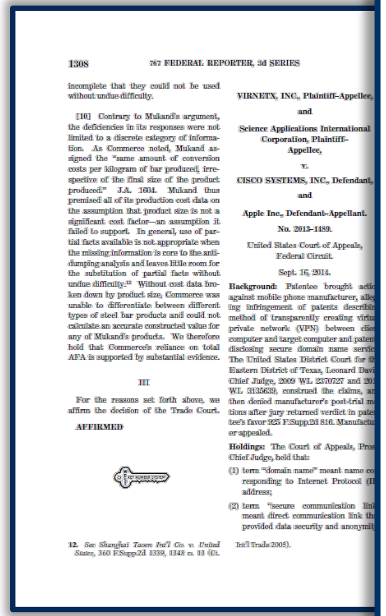
For at least the above reasons, we do not adopt Patent Owner’s proposed construction of the term “client computer” as a “user’s computer.” Instead, we construe the term “client computer,” under a broadest reasonable standard, to include a computer associated with a client.

Final Written Decision (Paper 42) at 9
135 Reply at 3
151 Reply at 3

The Federal Circuit Upheld Denial of JMOL

It Did Not Find Kiuchi's User Agent Is the Client

VirnetX v. Cisc
(Fed. Cir. 2014



1308 767 FEDERAL REPORTER, 3d SERIES

incomplete that they could not be used without undue difficulty.

[10] Contrary to Mukand's argument, the deficiencies in its responses were not limited to a discrete category of information. As Commerce noted, Mukand assigned the "same amount of conversion costs per kilogram of bar produced, irrespective of the final size of the product produced." J.A. 1604. Mukand thus premised all of its production cost data on the assumption that product size is not a significant cost factor—an assumption it failed to support. In general, use of partial facts available is not appropriate when the missing information is core to the anti-dumping analysis and leaves little room for the substitution of partial facts without undue difficulty.[12] Without cost data broken down by product size, Commerce was unable to differentiate between different types of steel bar products and could not calculate an accurate constructed value for any of Mukand's products. We therefore hold that Commerce's reliance on total AFA is supported by substantial evidence.

III

For the reasons set forth above, we affirm the decision of the Trade Court.

AFFIRMED

[12] *See Shanghai Taoen Int'l Co. v. United States*, 360 F.Supp.2d 1339, 1348 n. 13 (Ct. Int'l Trade 2005).

VIRNETX, INC., Plaintiff–Appellee,

and

Science Applications International Corporation, Plaintiff–Appellee,

v.

CISCO SYSTEMS, INC., Defendant,

and

Apple Inc., Defendant–Appellant.

No. 2013–1489.

United States Court of Appeals, Federal Circuit.

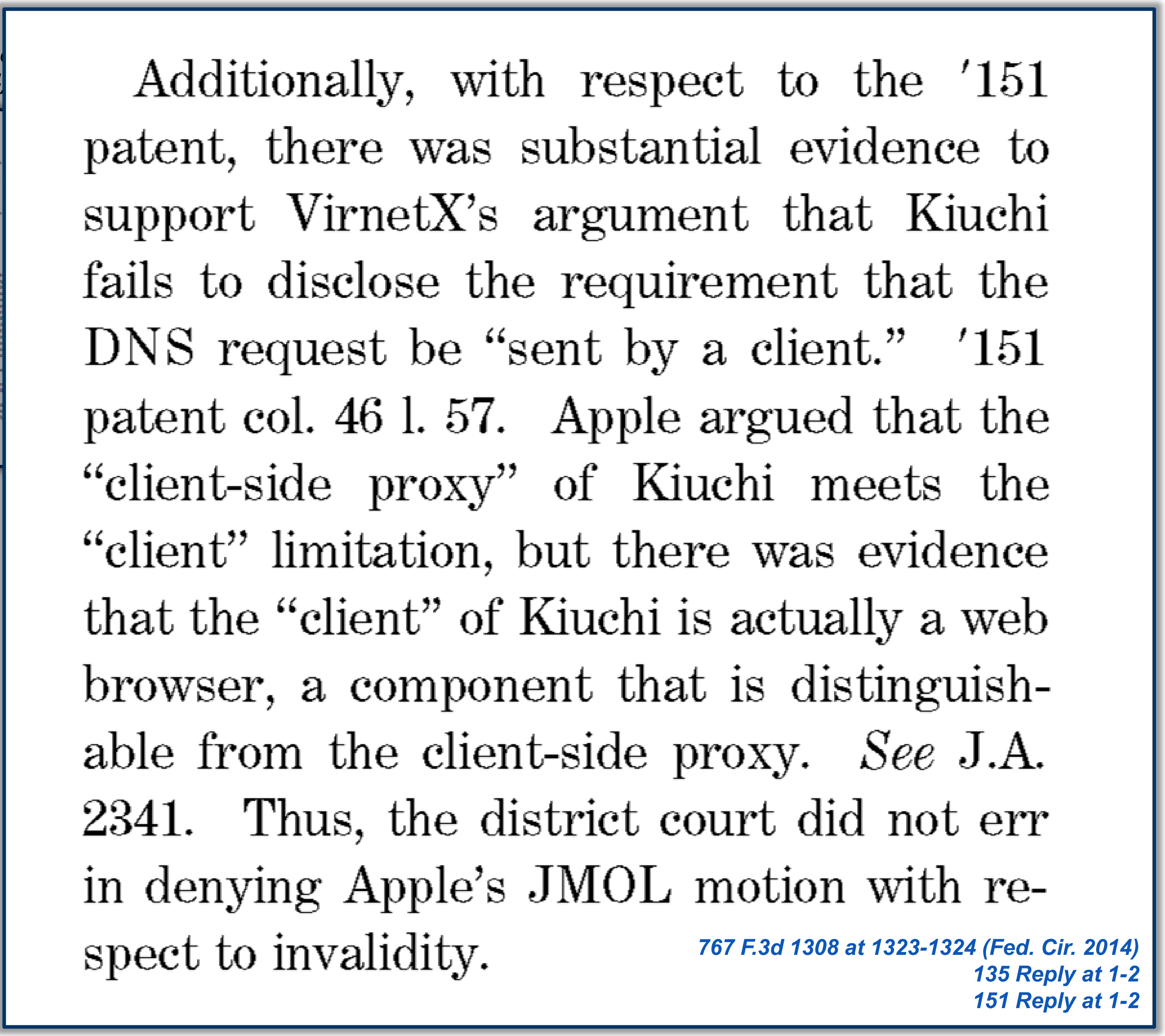
Sept. 16, 2014.

Background: Patentee brought actio against mobile phone manufacturer, alleg ing infringement of patents describin method of transparently creating virtu private network (VPN) between clien computer and target computer and patent disclosing secure domain name servic The United States District Court for th Eastern District of Texas, Leonard Davi Chief Judge, 2009 WL 2370727 and 201 WL 3135639, construed the claims, an then denied manufacturer's post-trial mo tions after jury returned verdict in paten tee's favor 925 F.Supp.2d 816. Manufactur er appealed.

Holdings: The Court of Appeals, Pros Chief Judge, held that:

(1) term "domain name" meant name co responding to Internet Protocol (IP address;

(2) term "secure communication link meant direct communication link th provided data security and anonymit



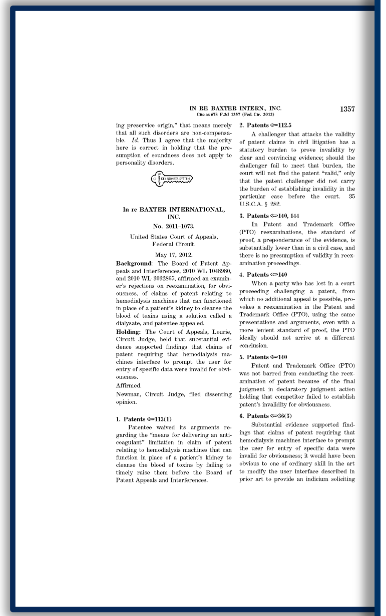
Additionally, with respect to the '151 patent, there was substantial evidence to support VirnetX's argument that Kiuchi fails to disclose the requirement that the DNS request be "sent by a client." '151 patent col. 46 l. 57. Apple argued that the "client-side proxy" of Kiuchi meets the "client" limitation, but there was evidence that the "client" of Kiuchi is actually a web browser, a component that is distinguishable from the client-side proxy. *See* J.A. 2341. Thus, the district court did not err in denying Apple's JMOL motion with respect to invalidity.

767 F.3d 1308 at 1323-1324 (Fed. Cir. 2014)
135 Reply at 1-2
151 Reply at 1-2

Different Legal Standards and a Different Record

In re Baxter Intern., Inc., 678 F.3d 1357 (Fed. Cir. 2012)

***In re Baxter* (Fed. Cir. 2012)**



IN RE BAXTER INTERN., INC. 1357
Cite as 678 F.3d 1357 (Fed. Cir. 2012)

ing preservice origin," that means merely that all such disorders are non-compensable. *Id.* Thus I agree that the majority here is correct in holding that the presumption of soundness does not apply to personality disorders.

In re BAXTER INTERNATIONAL, INC.

No. 2011–1073.

United States Court of Appeals,
Federal Circuit.

May 17, 2012.

Background: The Board of Patent Appeals and Interferences, 2010 WL 1048980, and 2010 WL 3032865, affirmed an examiner's rejections on reexamination, for obviousness, of claims of patent relating to hemodialysis machines that can functioned in place of a patient's kidney to cleanse the blood of toxins using a solution called a dialysate, and patentee appealed.

Holding: The Court of Appeals, Lourie, Circuit Judge, held that substantial evidence supported findings that claims of patent requiring that hemodialysis machines interface to prompt the user for entry of specific data were invalid for obviousness.

Affirmed.

Newman, Circuit Judge, filed dissenting opinion.

1. Patents ⚿113(1)

Patentee waived its arguments regarding the "means for delivering an anticoagulant" limitation in claim of patent relating to hemodialysis machines that can function in place of a patient's kidney to cleanse the blood of toxins by failing to timely raise them before the Board of Patent Appeals and Interferences.

2. Patents ⚿112.5

A challenger that attacks the validity of patent claims in civil litigation has a statutory burden to prove invalidity by clear and convincing evidence; should the challenger fail to meet that burden, the court will not find the patent "valid," only that the patent challenger did not carry the burden of establishing invalidity in the particular case before the court. 35 U.S.C.A. § 282.

3. Patents ⚿140, 144

In Patent and Trademark Office (PTO) reexaminations, the standard of proof, a preponderance of the evidence, is substantially lower than in a civil case, and there is no presumption of validity in reexamination proceedings.

4. Patents ⚿140

When a party who has lost in a court proceeding challenging a patent, from which no additional appeal is possible, provokes a reexamination in the Patent and Trademark Office (PTO), using the same presentations and arguments, even with a more lenient standard of proof, the PTO ideally should not arrive at a different conclusion.

5. Patents ⚿140

Patent and Trademark Office (PTO) was not barred from conducting the reexamination of patent because of the final judgment in declaratory judgment action holding that competitor failed to establish patent's invalidity for obviousness.

6. Patents ⚿36(3)

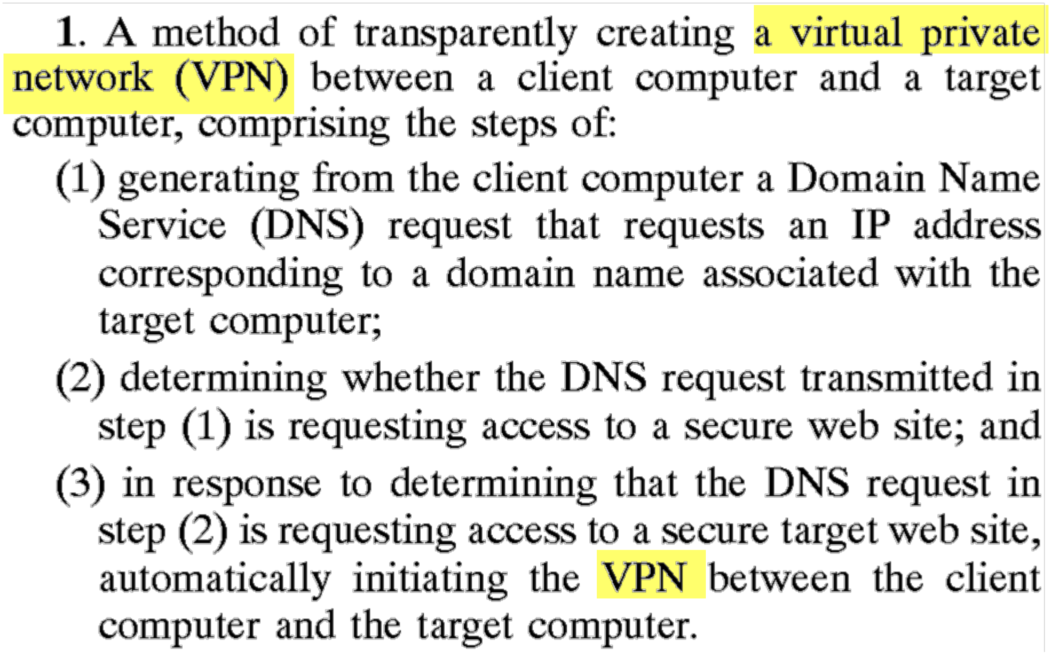
Substantial evidence supported findings that claims of patent requiring that hemodialysis machines interface to prompt the user for entry of specific data were invalid for obviousness; it would have been obvious to one of ordinary skill in the art to modify the user interface described in prior art to provide an indicium soliciting

More fundamentally, the PTO in reexamination proceedings and the court system in patent infringement actions "take different approaches in determining validity and on the same evidence could quite correctly come to different conclusions." *Swanson*, 540 F.3d at 1377 (*quoting Ethicon*, 849 F.2d at 1428). In particular, a challenger that attacks the validity of patent claims in civil litigation has a statutory burden to prove invalidity by clear and convincing evidence. *Id.* (*citing* 35 U.S.C. § 282); *see also Microsoft Corp. v. i4i Ltd.*, ___ U.S. ___, 131 S.Ct. 2238, 2242, 180 L.Ed.2d 131 (2011). Should the challenger fail to meet that burden, the court will not find the patent "valid," only that "the patent challenger did not carry the 'burden of establishing invalidity in the particular case before the court.'" *Swanson*, 540 F.3d at 1377 (*quoting Ethicon*, 849 F.2d at 1429 n. 3 (internal citations omitted)). In contrast, in PTO reexaminations "the standard of proof — a preponderance of the evidence — is substantially lower than in a civil case" and there is no presumption of validity in reexamination proceedings. *Id.* at 1378.

678 F.3d at 1364
135 Reply at 2
151 Reply at 2

135 Patent: VPN

135 Patent Claim 1



1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

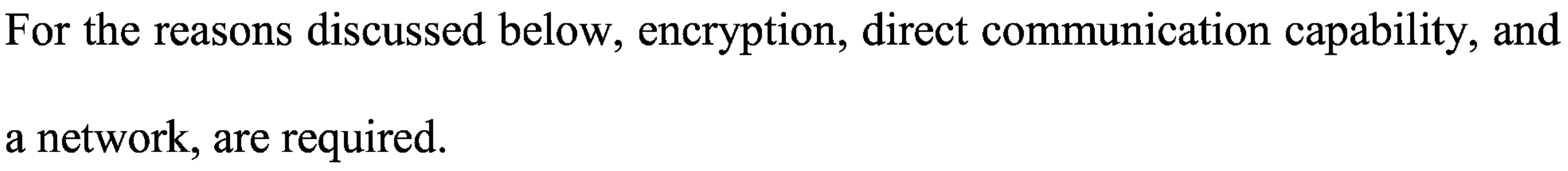
(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

VPN

Petitioners' Construction	Patent Owner's Construction
A secure network that includes portions of a public network	A network of computers which privately and directly communicate with each other by encrypting traffic over insecure communication paths between the computers

135 Petition at 7; Resp. at 4

Patent Owner's Construction



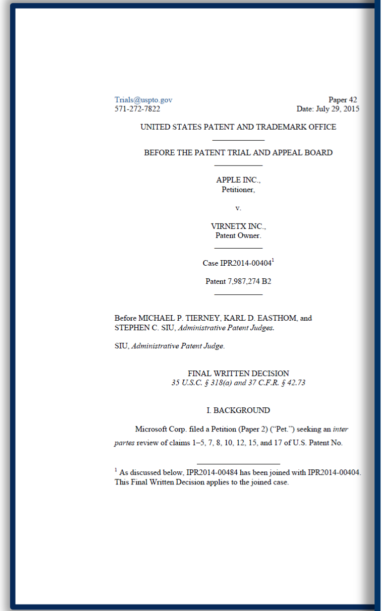
For the reasons discussed below, encryption, direct communication capability, and a network, are required.

135 PO Resp. at 5

IPR2014-00404: VPN Communication Link

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404 Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

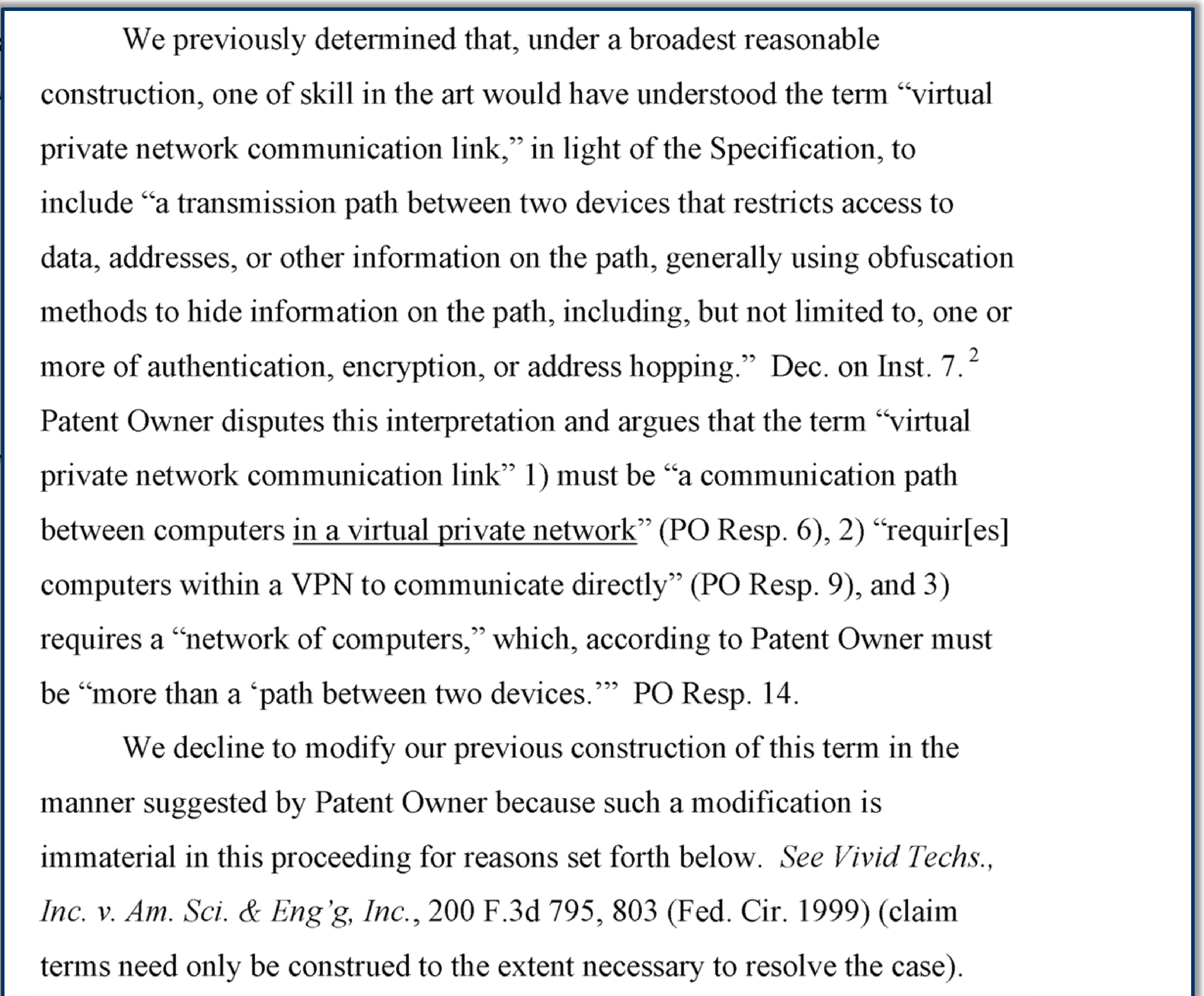
SIU, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Microsoft Corp. filed a Petition (Paper 2) ("Pet.") seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

[1] As discussed below, IPR2014-00484 has been joined with IPR2014-00404. This Final Written Decision applies to the joined case.



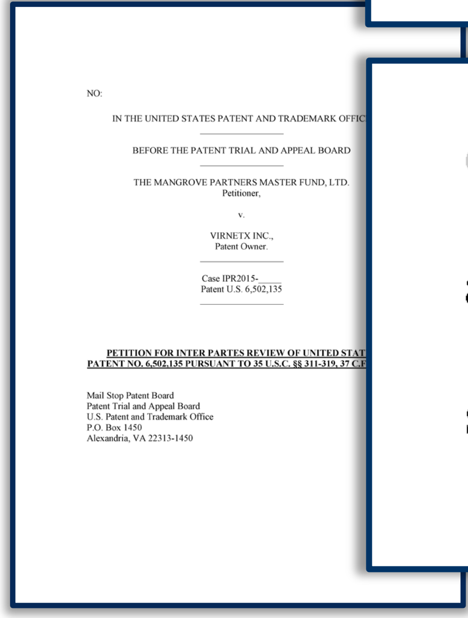
We previously determined that, under a broadest reasonable construction, one of skill in the art would have understood the term "virtual private network communication link," in light of the Specification, to include "a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." Dec. on Inst. 7.[2] Patent Owner disputes this interpretation and argues that the term "virtual private network communication link" 1) must be "a communication path between computers in a virtual private network" (PO Resp. 6), 2) "requir[es] computers within a VPN to communicate directly" (PO Resp. 9), and 3) requires a "network of computers," which, according to Patent Owner must be "more than a 'path between two devices.'" PO Resp. 14.

We decline to modify our previous construction of this term in the manner suggested by Patent Owner because such a modification is immaterial in this proceeding for reasons set forth below. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (claim terms need only be construed to the extent necessary to resolve the case).

Final Written Decision (Paper 42) at 4; 135 Reply at 3; 151 Reply at 3

Kiuchi: Encryption

Petition
Paper 5



NO:

IN THE UNITED STATES PATENT AND TRADEMARK OFFIC

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD.
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-_____
Patent U.S. 6,502,135

PETITION FOR INTER PARTES REVIEW OF UNITED STAT
PATENT NO. 6,502,135 PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F

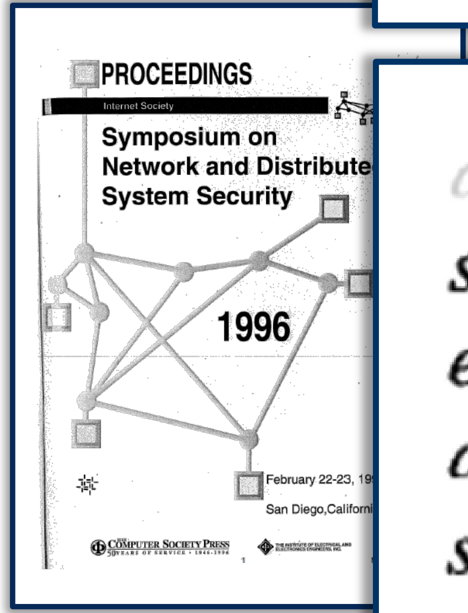
Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Petition

connection is established. *See id.* Data is securely transmitted between the user agent and origin server because the proxy servers automatically encrypt any traffic sent between them. *See* Ex. 1002, p. 65, § 1; *see also* Ex. 1003, ¶ 26. The connect

135 Pet. at 29

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



PROCEEDINGS

Internet Society

Symposium on
Network and Distribute
System Security

1996

February 22-23, 19

San Diego,Californi

COMPUTER SOCIETY PRESS
50 YEARS OF SERVICE • 1946-1996

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

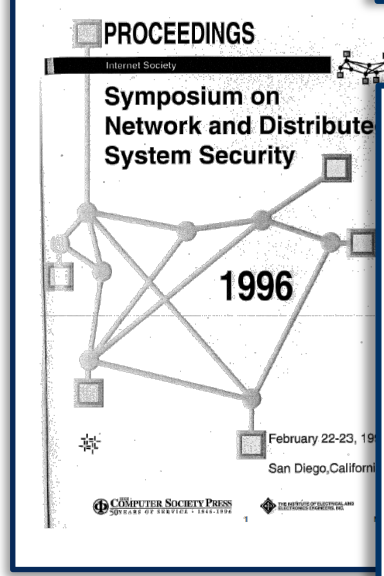
a C-HTTP name server. A client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol while communications between a user agent and client-side proxy or an origin server and server-side proxy are performed using current HTTP/1.0.

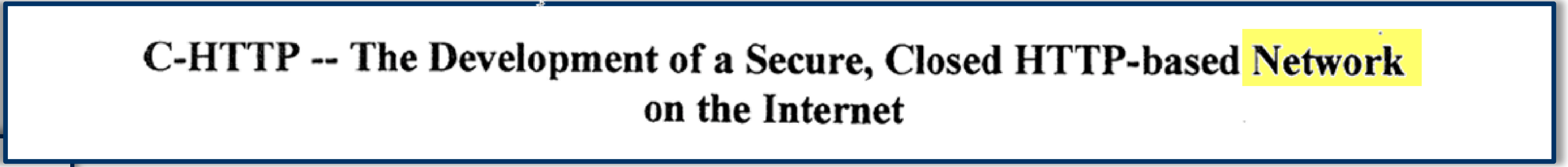
Kiuchi at 64; 135 Pet. at 26

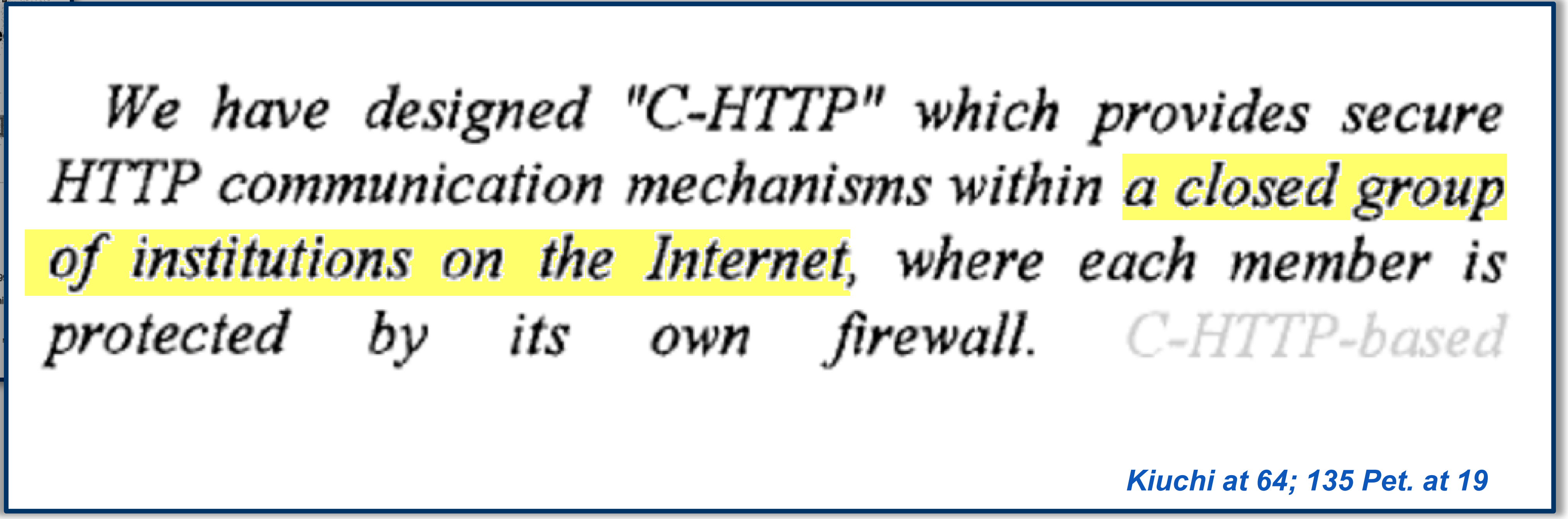
Kiuchi
Ex. 1002

Kiuchi: Network

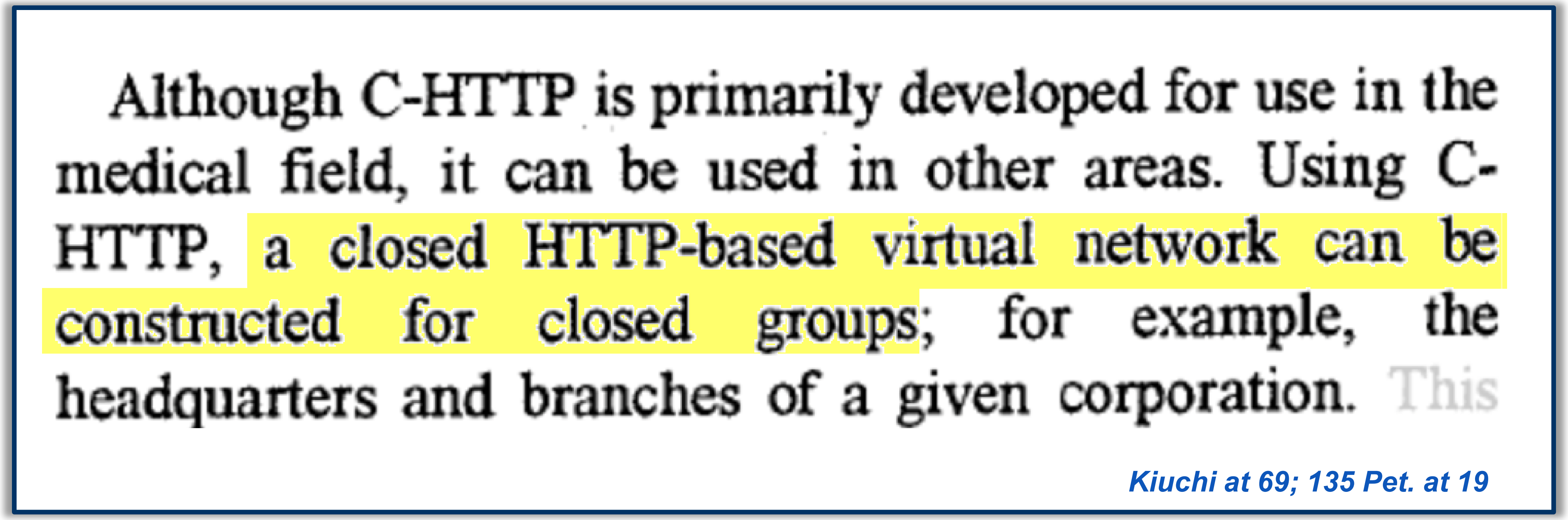
Kiuchi
Ex. 1002




C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet


We have designed "C-HTTP" which provides secure HTTP communication mechanisms within a closed group of institutions on the Internet, where each member is protected by its own firewall. C-HTTP-based

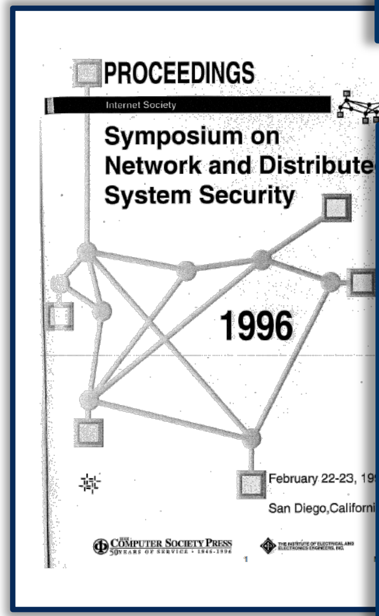
Kiuchi at 64; 135 Pet. at 19


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

Kiuchi at 69; 135 Pet. at 19

Kiuchi: Network

Kiuchi
Ex. 1002



PROCEEDINGS

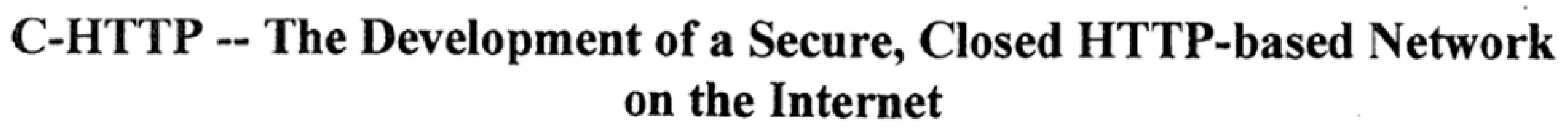
Internet Society

Symposium on
Network and Distribute
System Security

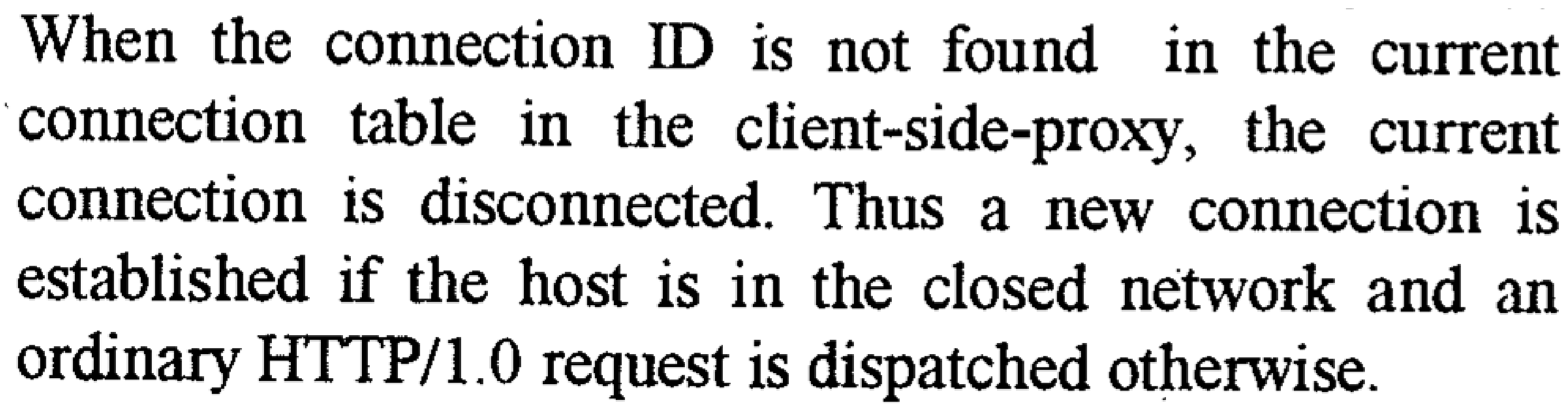
1996

February 22-23, 19
San Diego,Californi

Computer Society Press

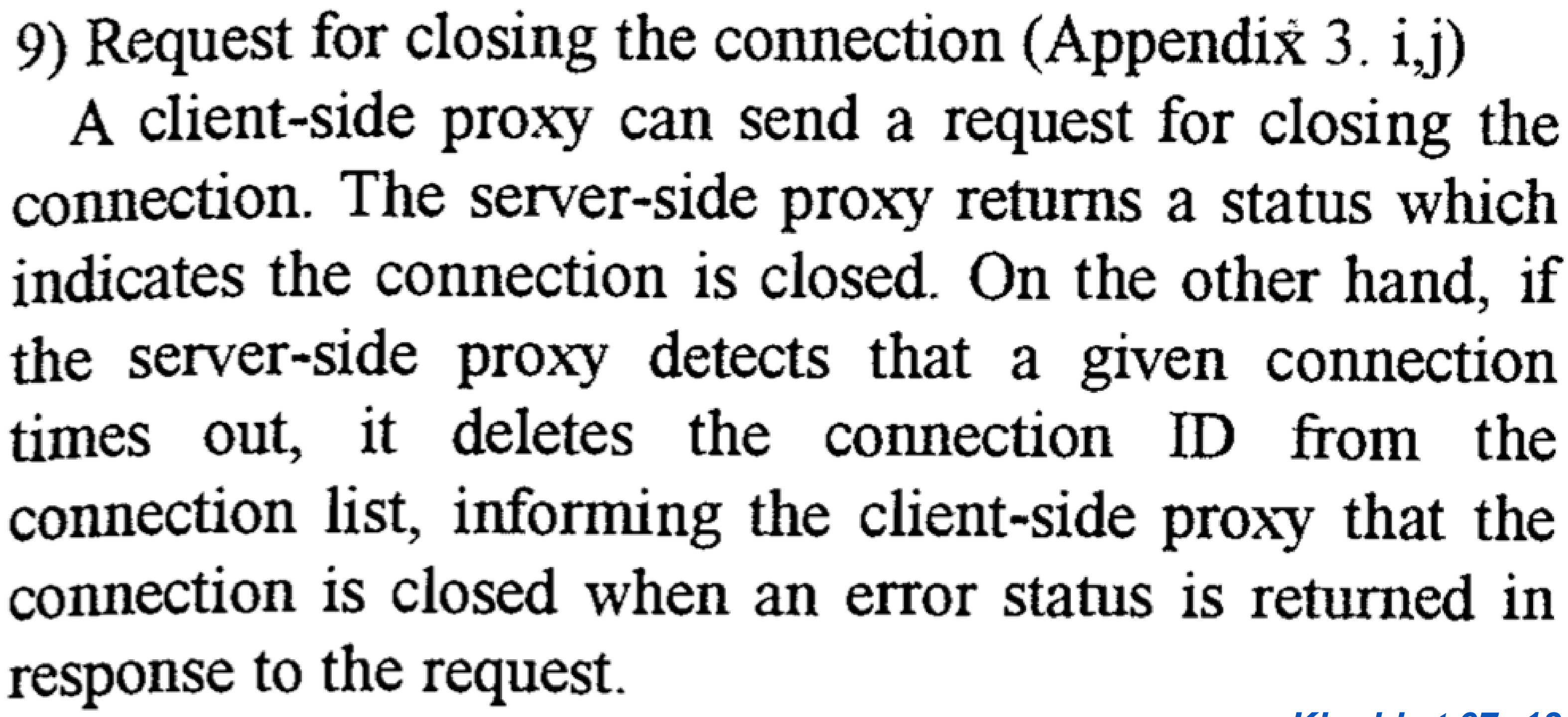


C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



When the connection ID is not found in the current connection table in the client-side-proxy, the current connection is disconnected. Thus a new connection is established if the host is in the closed network and an ordinary HTTP/1.0 request is dispatched otherwise.

Kiuchi at 65; 135 Pet. at 22



9) Request for closing the connection (Appendix 3. i,j)

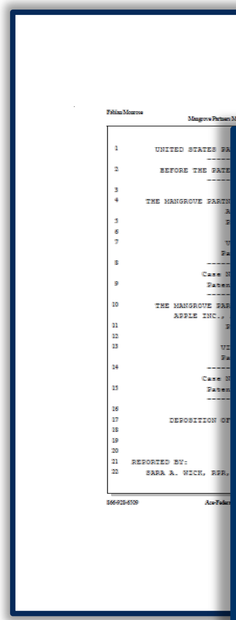
A client-side proxy can send a request for closing the connection. The server-side proxy returns a status which indicates the connection is closed. On the other hand, if the server-side proxy detects that a given connection times out, it deletes the connection ID from the connection list, informing the client-side proxy that the connection is closed when an error status is returned in response to the request.

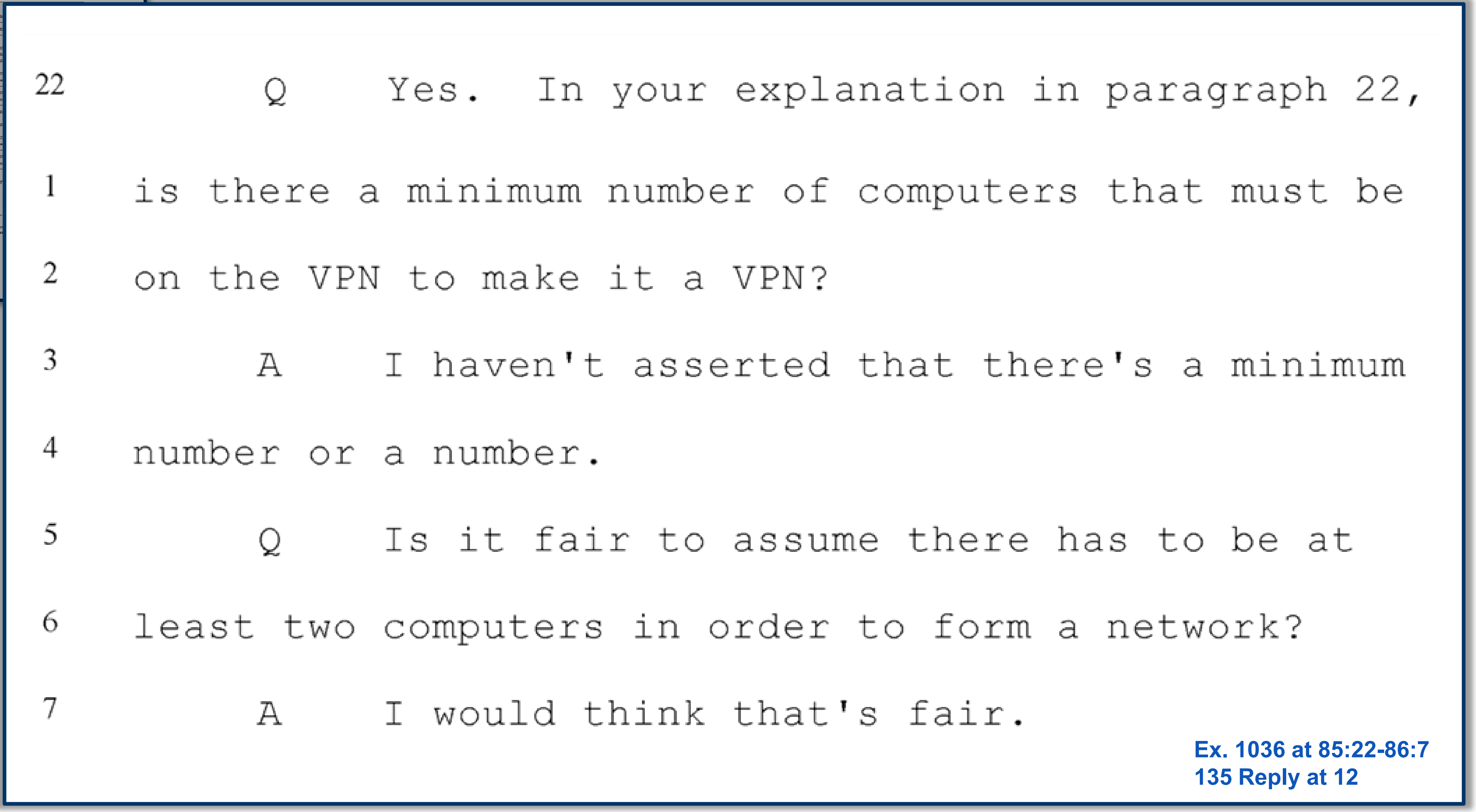
Kiuchi at 67; 135 Reply at 13

Dr. Monrose: Network

Ex. 1036 – Deposition Transcript of Dr. Fabian Monrose (April 28, 2016)

Monrose Dep. Ex. 1036





Q Yes. In your explanation in paragraph 22, is there a minimum number of computers that must be on the VPN to make it a VPN?

A I haven't asserted that there's a minimum number or a number.

Q Is it fair to assume there has to be at least two computers in order to form a network?

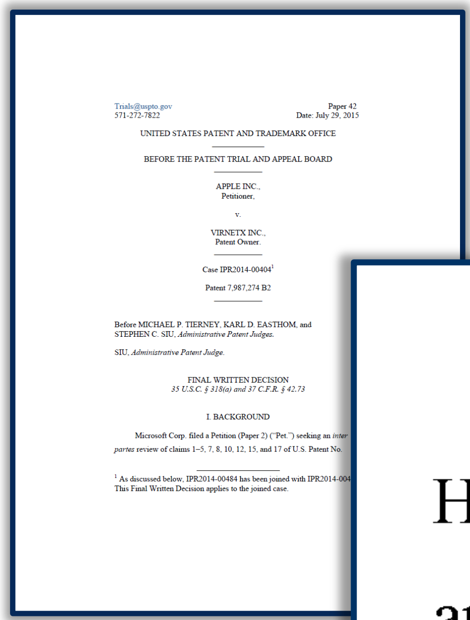
A I would think that's fair.

Ex. 1036 at 85:22-86:7
135 Reply at 12

IPR2014-00404: “Network”

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404
Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

SIU, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Microsoft Corp. filed a Petition (Paper 2) (“Pet.”) seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

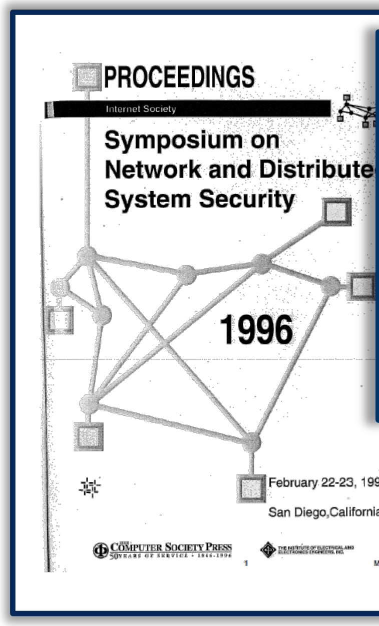
[1] As discussed below, IPR2014-00484 has been joined with IPR2014-004
This Final Written Decision applies to the joined case.

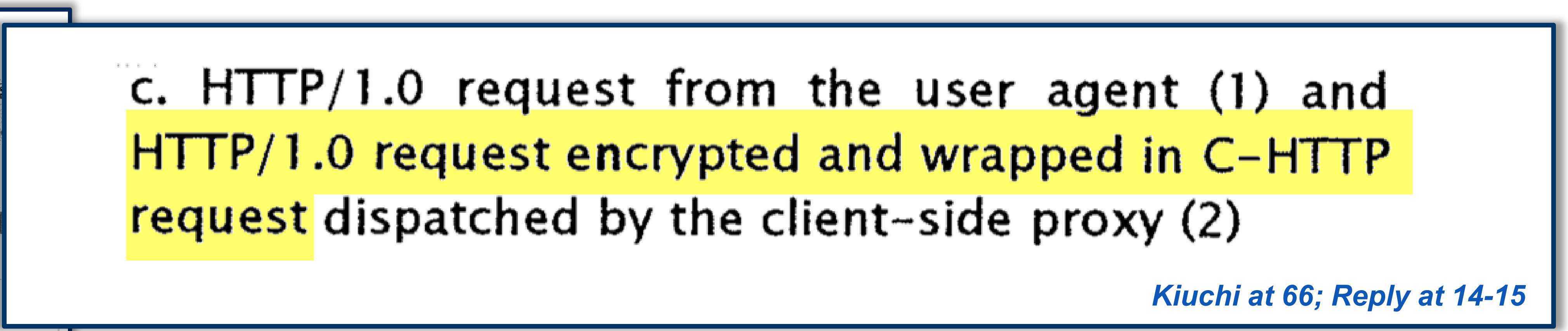
For example, Kiuchi discloses one embodiment of the use of a C-HTTP name server (and client-side and server-side proxies) in “networks among hospitals and related institutions.” Ex 1004, 64. At least in view of this explicit disclosure of “networks,” we are not persuaded by Patent Owner that Kiuchi fails to disclose a “network.”

Final Written Decision (Paper 42) at 14
135 Reply at 3, 13
151 Reply at 3

Kiuchi vs 135 Patent: Direct

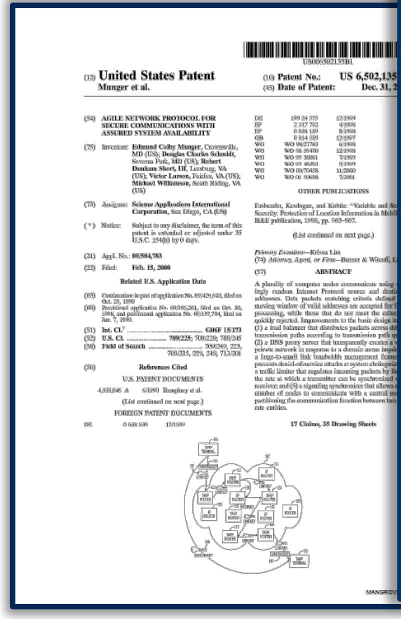
Kiuchi
Ex. 1002

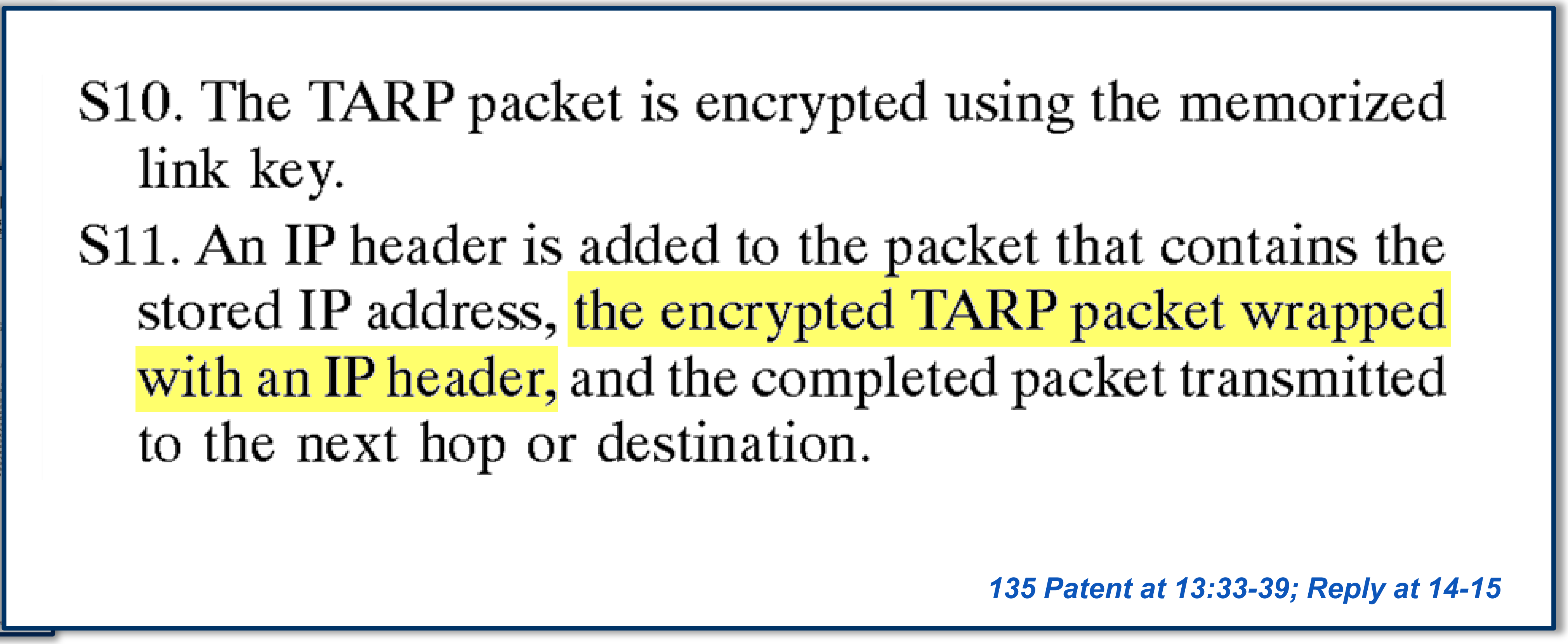




c. HTTP/1.0 request from the user agent (1) and HTTP/1.0 request encrypted and wrapped in C-HTTP request dispatched by the client-side proxy (2)

Kiuchi at 66; Reply at 14-15





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.

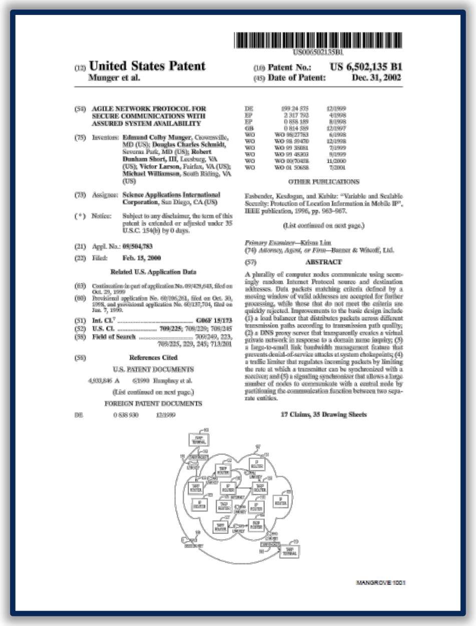
135 Patent at 13:33-39; Reply at 14-15

135 Patent
Ex. 1001

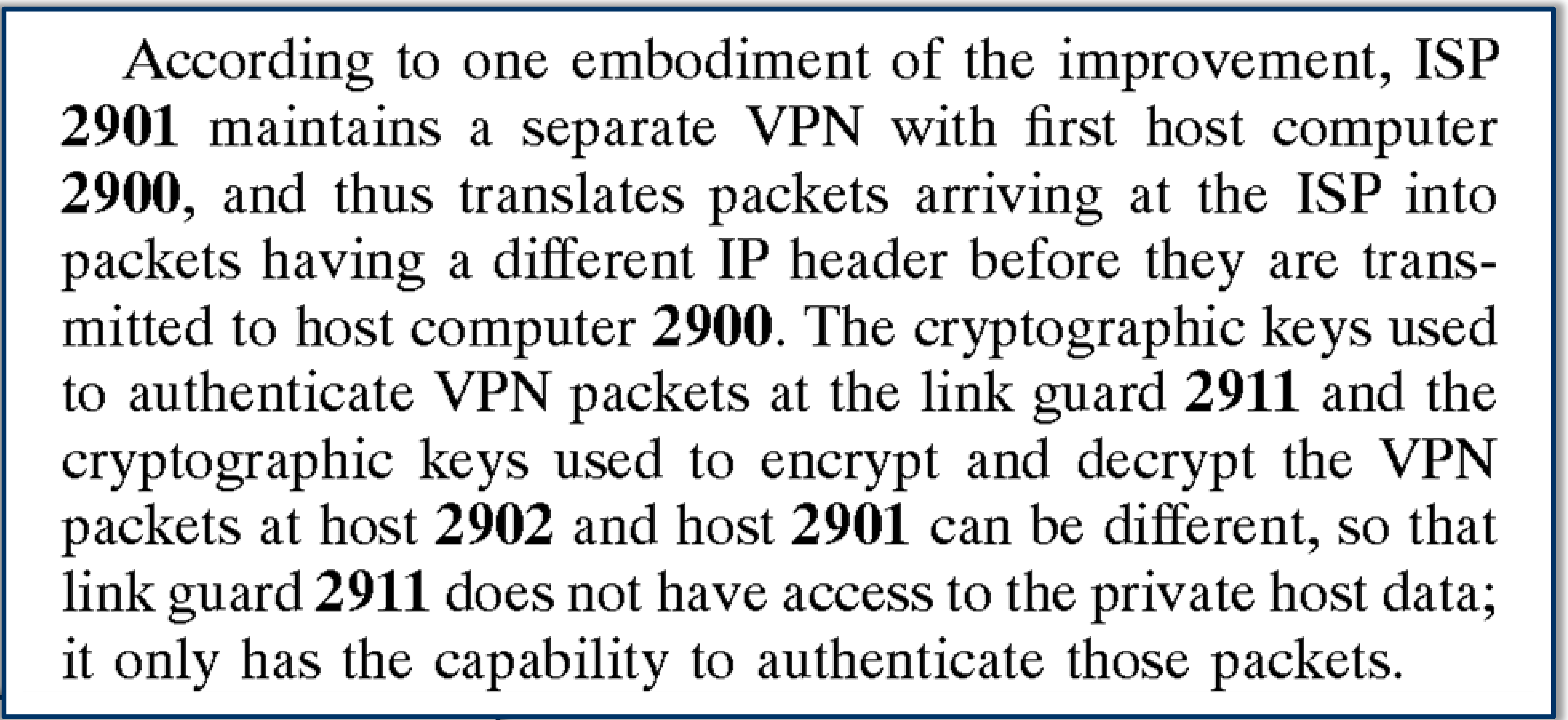
Claim Construction: Direct

Ex. 1001 – 135 Patent

135 Patent
Ex. 1001



United States Patent
Munger et al.
Patent No.: US 6,502,135 B1
Date of Patent: Dec. 31, 2002



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.

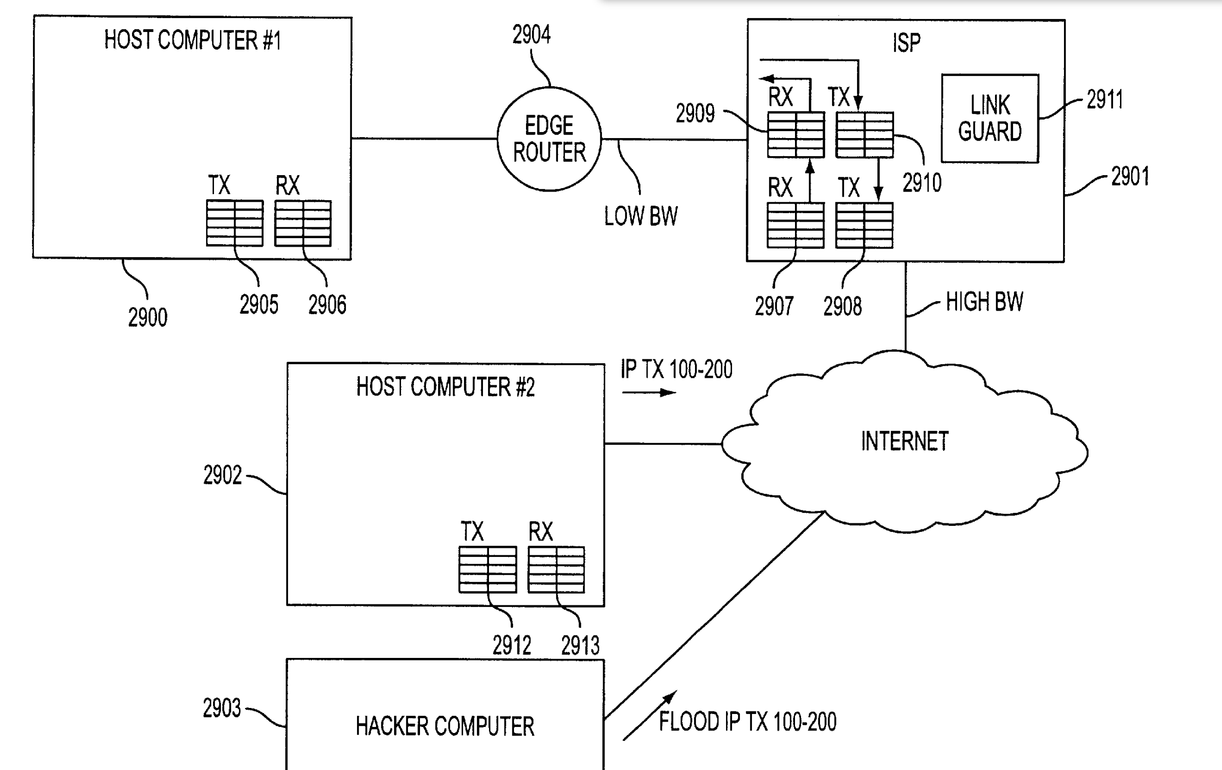


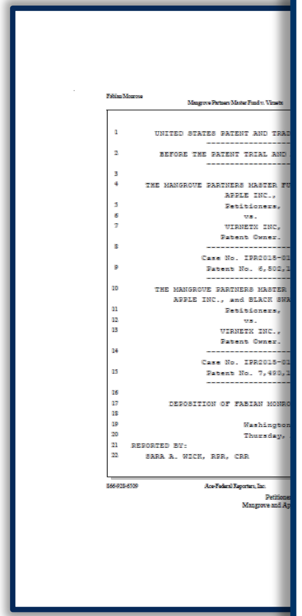
FIG. 29

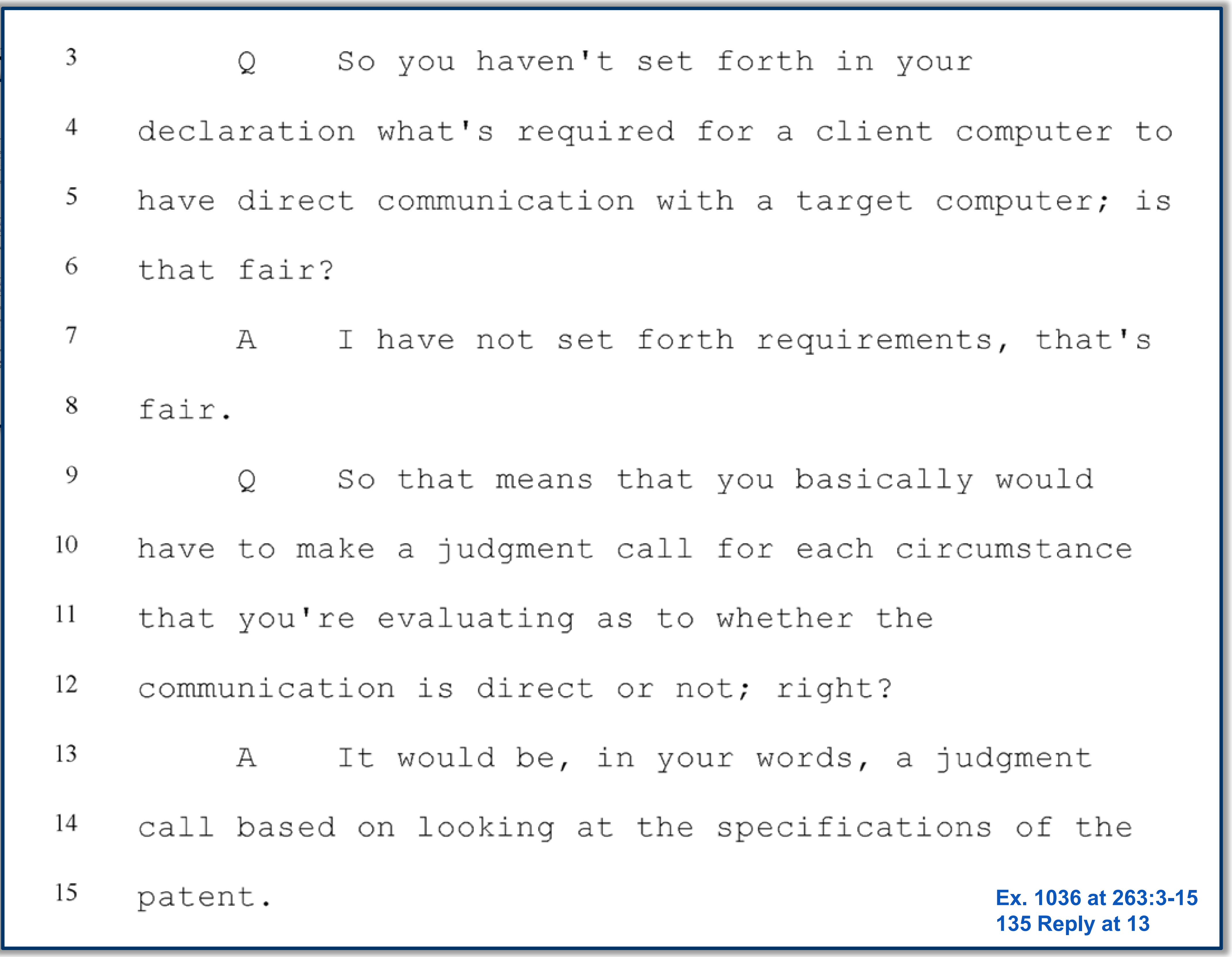
Ex. 1001 at 41:56-65, Fig. 29;
135 PO Resp. at 8;
135 Reply at 14

Dr. Monrose Did Not Know What "Direct" Requires

Ex. 1036 – Deposition Transcript of Dr. Fabian Monrose (April 28, 2016)

Monrose Ex. 10





Q So you haven't set forth in your declaration what's required for a client computer to have direct communication with a target computer; is that fair?

A I have not set forth requirements, that's fair.

Q So that means that you basically would have to make a judgment call for each circumstance that you're evaluating as to whether the communication is direct or not; right?

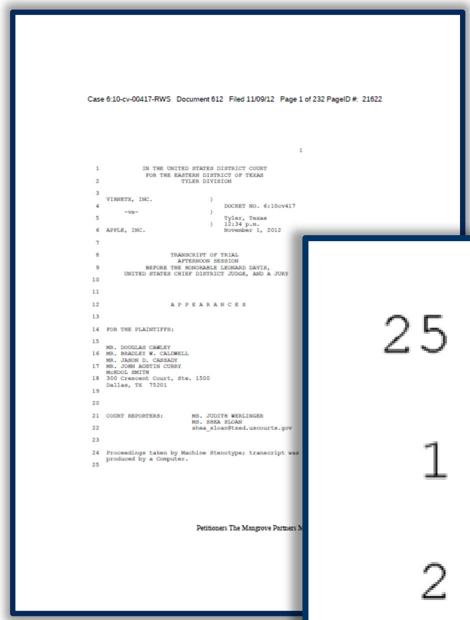
A It would be, in your words, a judgment call based on looking at the specifications of the patent.

Ex. 1036 at 263:3-15
135 Reply at 13

VirnetX's Litigation Position: "Direct" Means "Direct Addressability"

Ex. 1044 –Transcript of Trial, Afternoon Session (E.D. Tex. Nov. 1, 2012)

Trial Transcript
Ex. 1044



Case 6:10-cv-00417-RWS Document 612 Filed 11/09/12 Page 1 of 232 PageID #: 21622

1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX, INC.)
DOCKET NO. 6:10cv417
-vs-)
Tyler, Texas
) 12:34 p.m.
APPLE, INC. November 1, 2012

TRANSCRIPT OF TRIAL
AFTERNOON SESSION
BEFORE THE HONORABLE LEONARD DAVIS,
UNITED STATES CHIEF DISTRICT JUDGE, AND A JURY

APPEARANCES

FOR THE PLAINTIFFS:

MR. DOUGLAS CAWLEY
MR. BRADLEY W. CALDWELL
MR. JASON D. CASSADY
MR. JOHN AUSTIN CURRY
McKOOL SMITH
300 Crescent Court, Ste. 1500
Dallas, TX 75201

COURT REPORTERS: MS. JUDITH WERLINGER
MS. SHEA SLOAN
shea_sloan@txed.uscourts.gov

Proceedings taken by Machine Stenotype; transcript was produced by a Computer.

Petitioners The Mangrove Partners M

Q. (By Mr. Williams) This is Judge Davis' construction. A secure communication link must be a direct communication link.

And I believe that you've told us that direct communication refers to direct addressability, correct?

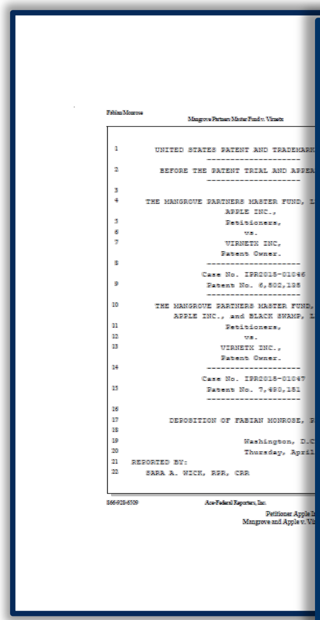
A. That's correct.

Ex. 1044 at 50:25-51:5
135 Reply at 16

Dr. Monrose: Kiuchi's URL Contains the Actual Address of the Resource on Origin Server

Ex. 1036 – Deposition Transcript of Dr. Fabian Monrose (April 28, 2016)

Monrose Dep. Ex. 1036



Fabian Monrose

Mangrove Partners Master Fund v. Virnetx

UNITED STATES PATENT AND TRADEMARK

BEFORE THE PATENT TRIAL AND APPEA

THE MANGROVE PARTNERS MASTER FUND, L
APPLE INC.,
Petitioners,
vs.
VIRNETX INC,
Patent Owner.

Case No. IPR2015-01046
Patent No. 6,502,135

THE MANGROVE PARTNERS MASTER FUND,
APPLE INC., and BLACK SWAMP, L
Petitioners,
vs.
VIRNETX INC.,
Patent Owner.

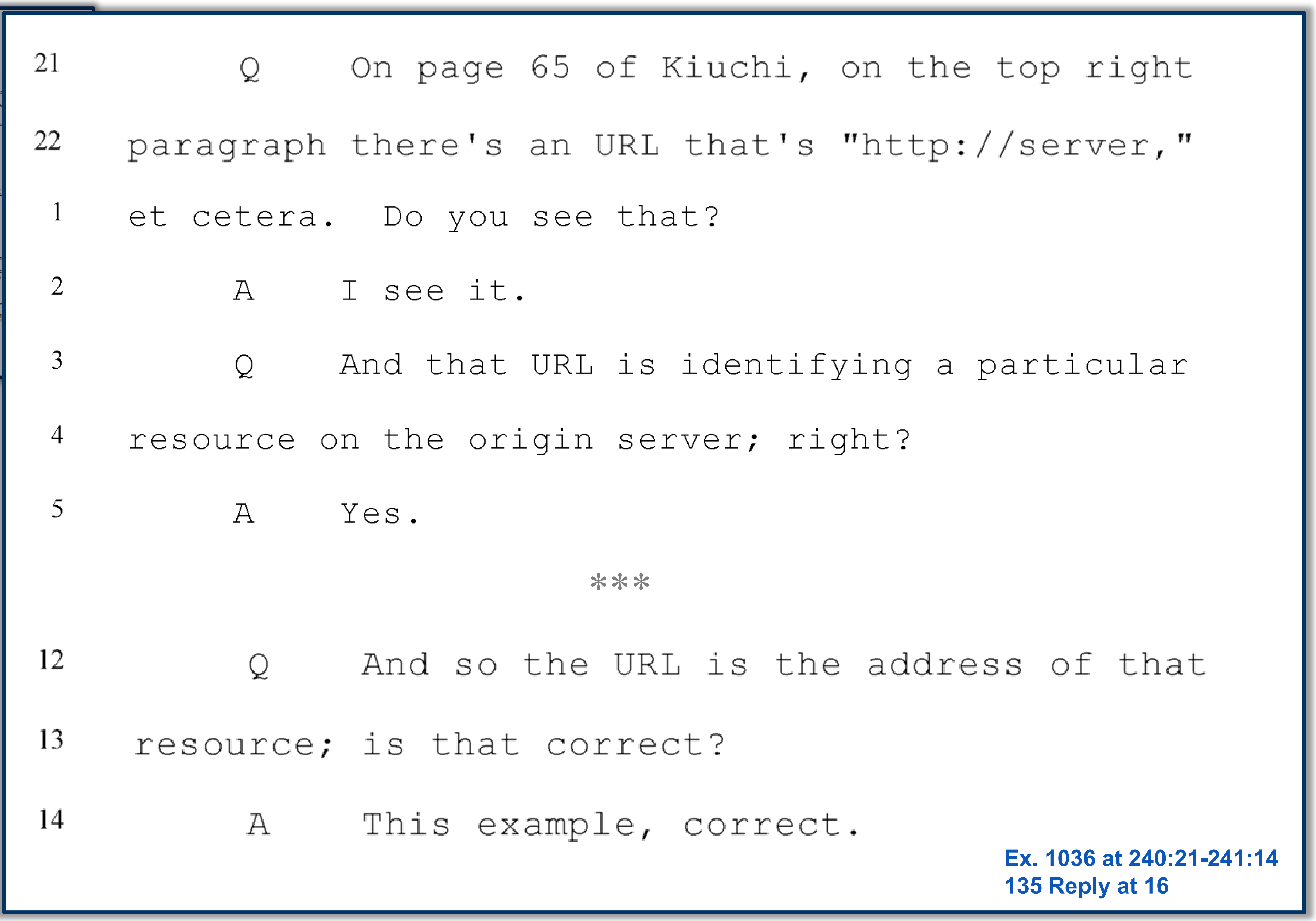
Case No. IPR2015-01047
Patent No. 7,490,151

DEPOSITION OF FABIAN MONROSE, P

Washington, D.C
Thursday, April
REPORTED BY:
SARA A. WICK, RPR, CRR

866-928-6509 Ace-Federal Reporters, Inc.

Petitioner Apple I
Mangrove and Apple v. Vi



Q On page 65 of Kiuchi, on the top right paragraph there's an URL that's "http://server," et cetera. Do you see that?

A I see it.

Q And that URL is identifying a particular resource on the origin server; right?

A Yes.

***

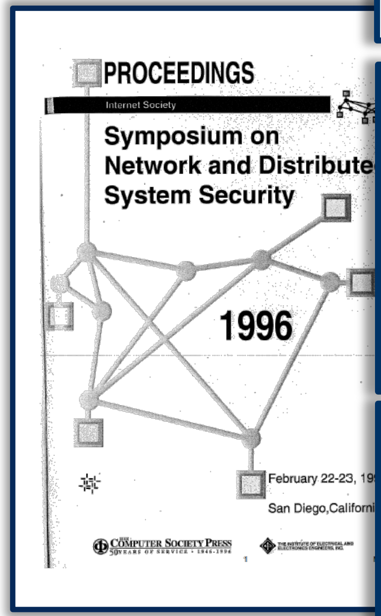
Q And so the URL is the address of that resource; is that correct?

A This example, correct.

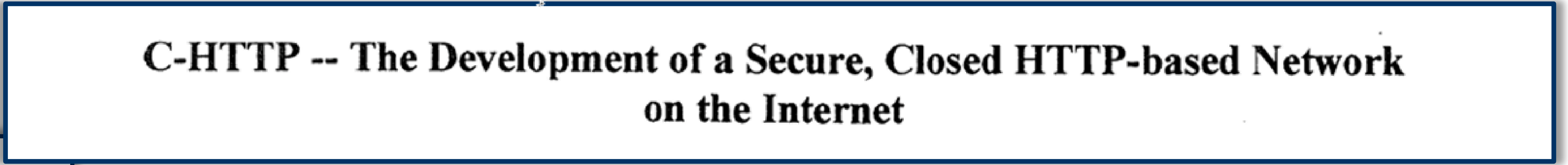
Ex. 1036 at 240:21-241:14
135 Reply at 16

Kiuchi: Direct

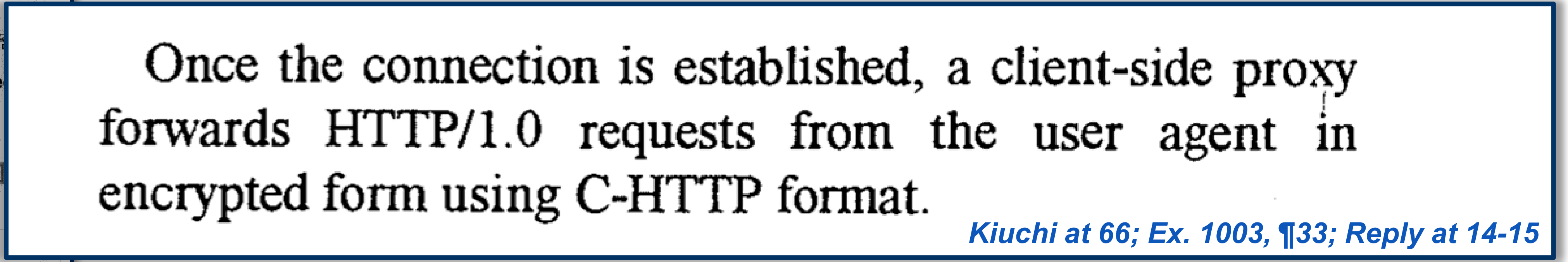
Kiuchi
Ex. 1002



PROCEEDINGS
Internet Society
Symposium on
Network and Distribute
System Security
1996
February 22-23, 19
San Diego,Californ
Computer Society Press

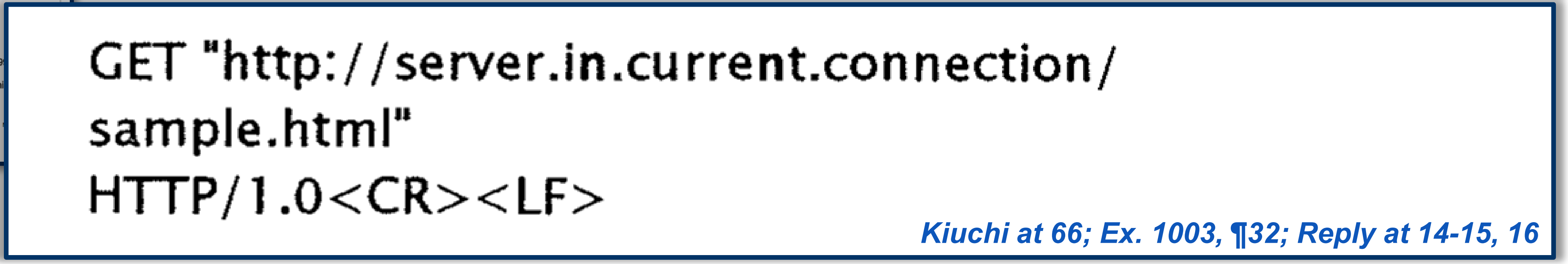


C-HTTP -- The Development of a Secure, Closed HTTP-based Network
on the Internet



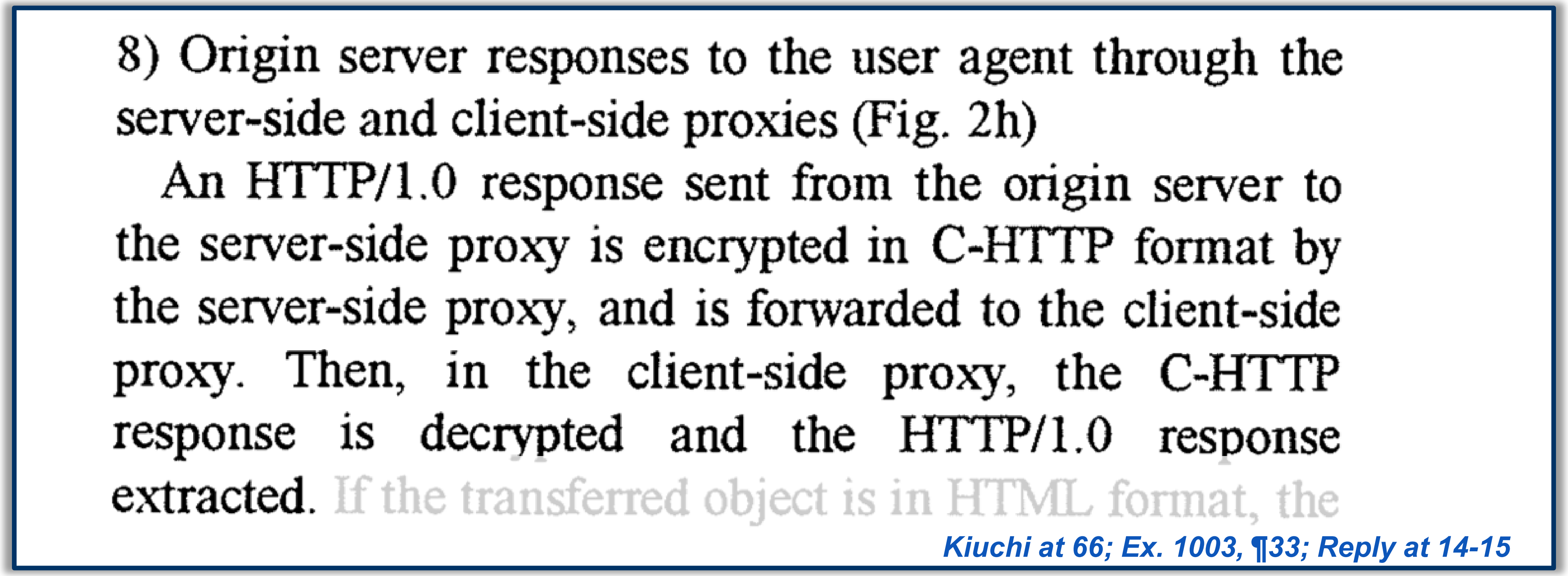
Once the connection is established, a client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format.

Kiuchi at 66; Ex. 1003, ¶33; Reply at 14-15



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

Kiuchi at 66; Ex. 1003, ¶32; Reply at 14-15, 16



8) Origin server responses to the user agent through the server-side and client-side proxies (Fig. 2h)

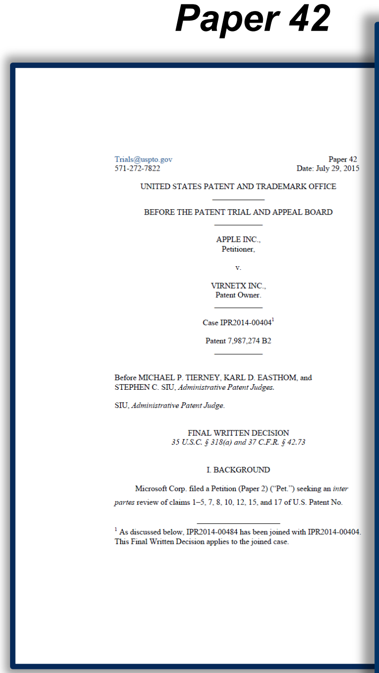
An HTTP/1.0 response sent from the origin server to the server-side proxy is encrypted in C-HTTP format by the server-side proxy, and is forwarded to the client-side proxy. Then, in the client-side proxy, the C-HTTP response is decrypted and the HTTP/1.0 response extracted. If the transferred object is in HTML format, the

Kiuchi at 66; Ex. 1003, ¶33; Reply at 14-15

IPR2014-00404: “Direct” Communications

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404
Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

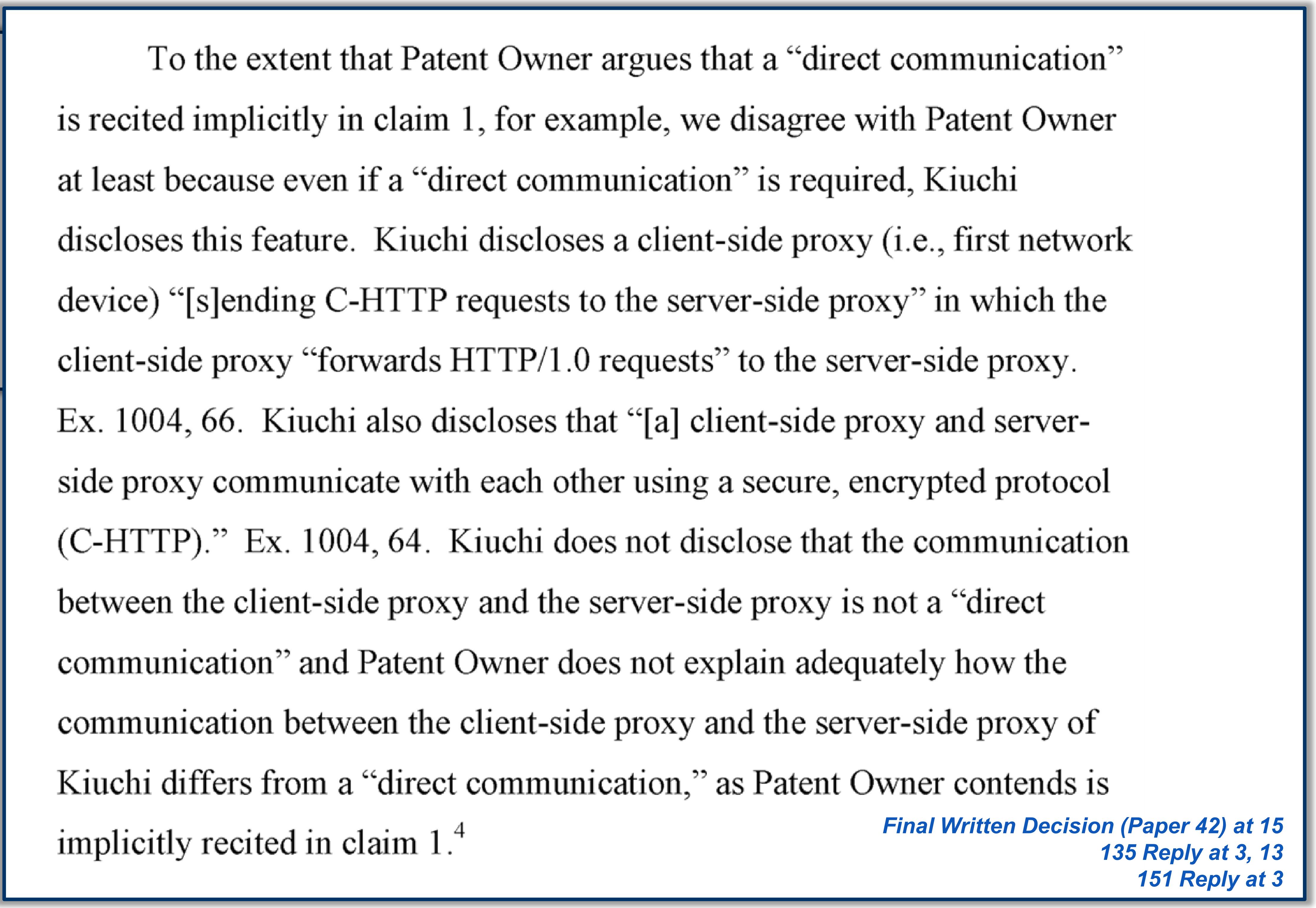
SIU, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Microsoft Corp. filed a Petition (Paper 2) (“Pet.”) seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

[1] As discussed below, IPR2014-00484 has been joined with IPR2014-00404. This Final Written Decision applies to the joined case.



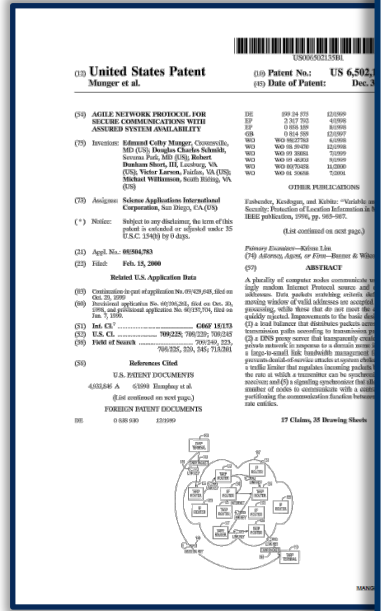
To the extent that Patent Owner argues that a “direct communication” is recited implicitly in claim 1, for example, we disagree with Patent Owner at least because even if a “direct communication” is required, Kiuchi discloses this feature. Kiuchi discloses a client-side proxy (i.e., first network device) “[s]ending C-HTTP requests to the server-side proxy” in which the client-side proxy “forwards HTTP/1.0 requests” to the server-side proxy. Ex. 1004, 66. Kiuchi also discloses that “[a] client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol (C-HTTP).” Ex. 1004, 64. Kiuchi does not disclose that the communication between the client-side proxy and the server-side proxy is not a “direct communication” and Patent Owner does not explain adequately how the communication between the client-side proxy and the server-side proxy of Kiuchi differs from a “direct communication,” as Patent Owner contends is implicitly recited in claim 1.[4]

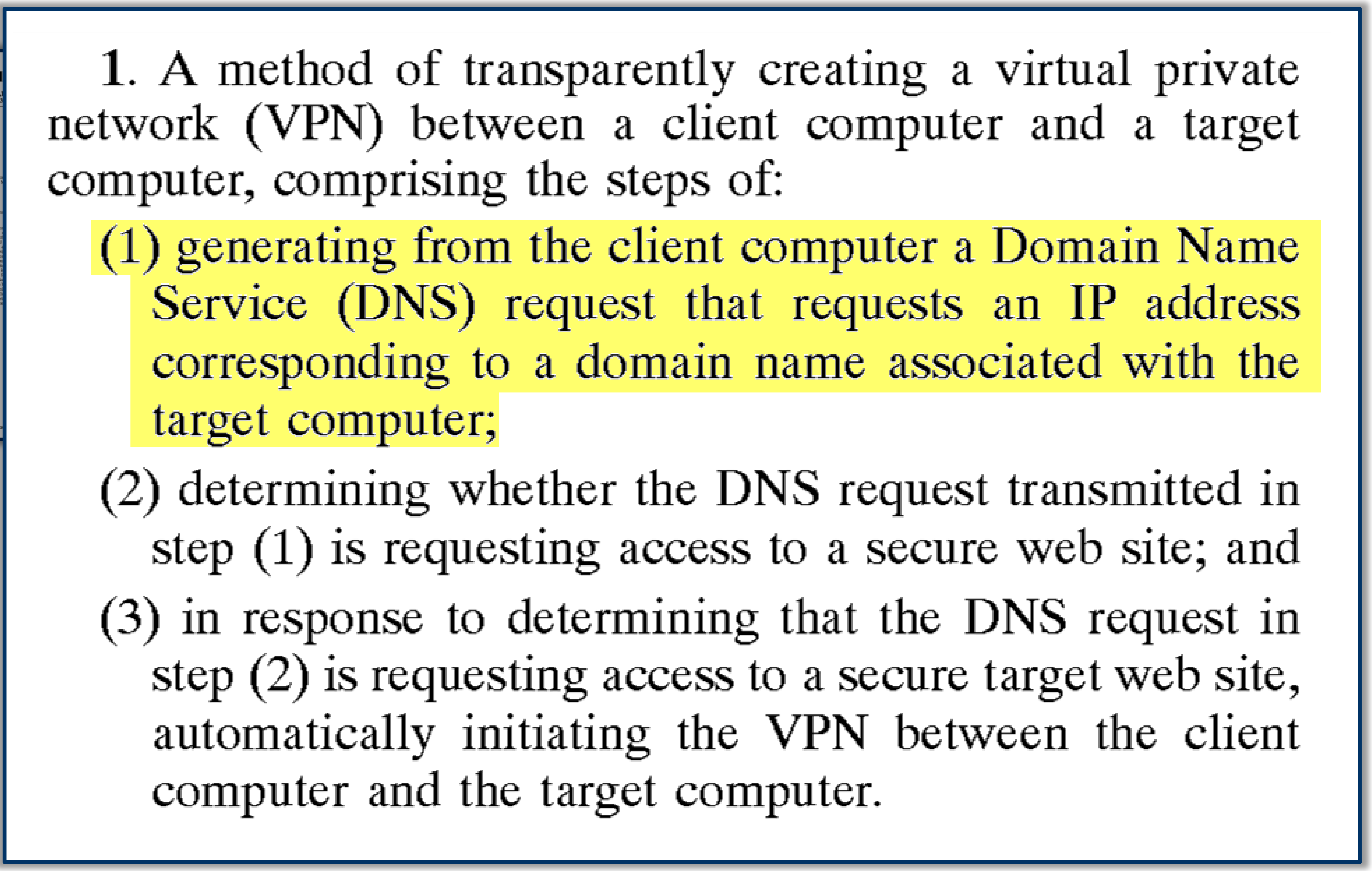
Final Written Decision (Paper 42) at 15
135 Reply at 3, 13
151 Reply at 3

135 Patent: Step 1

"generating from the client computer a [DNS] request"

135 Patent
Ex. 1001





1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

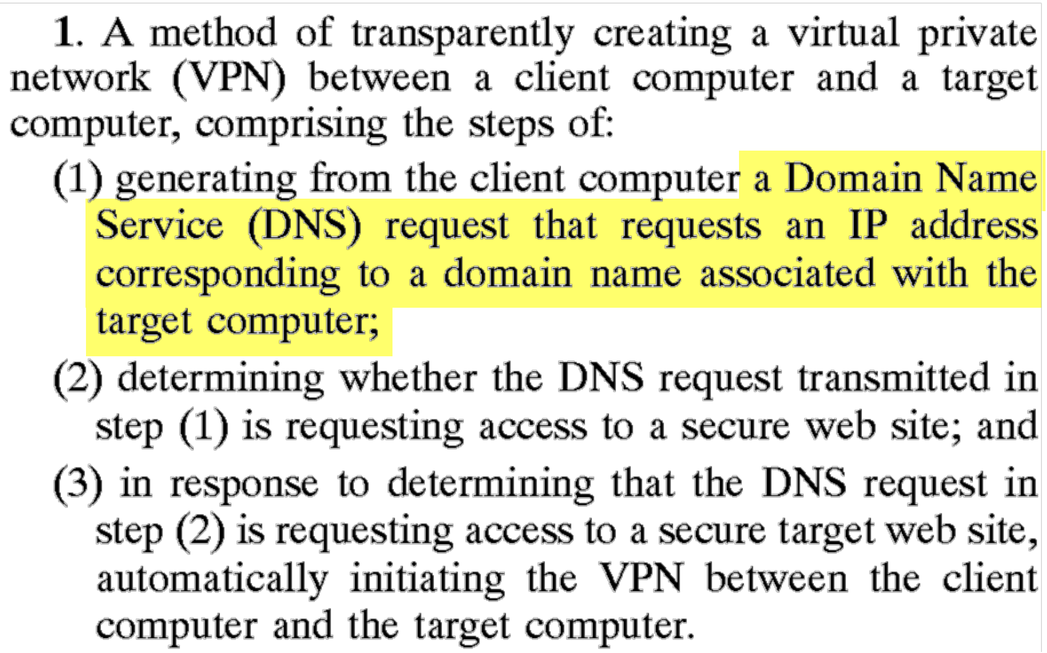
(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

135 Patent: DNS Request

Claim Construction

135 Patent Claim 1



1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

DNS Request

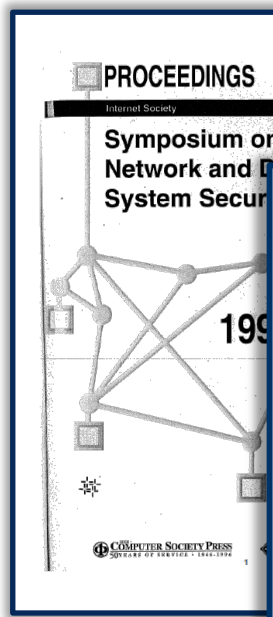
Petitioners' Construction	**Patent Owner's Construction**
A request for a resource corresponding to a network address	A request for a resource corresponding to a domain name

135 Petition at 14; Resp. at 13

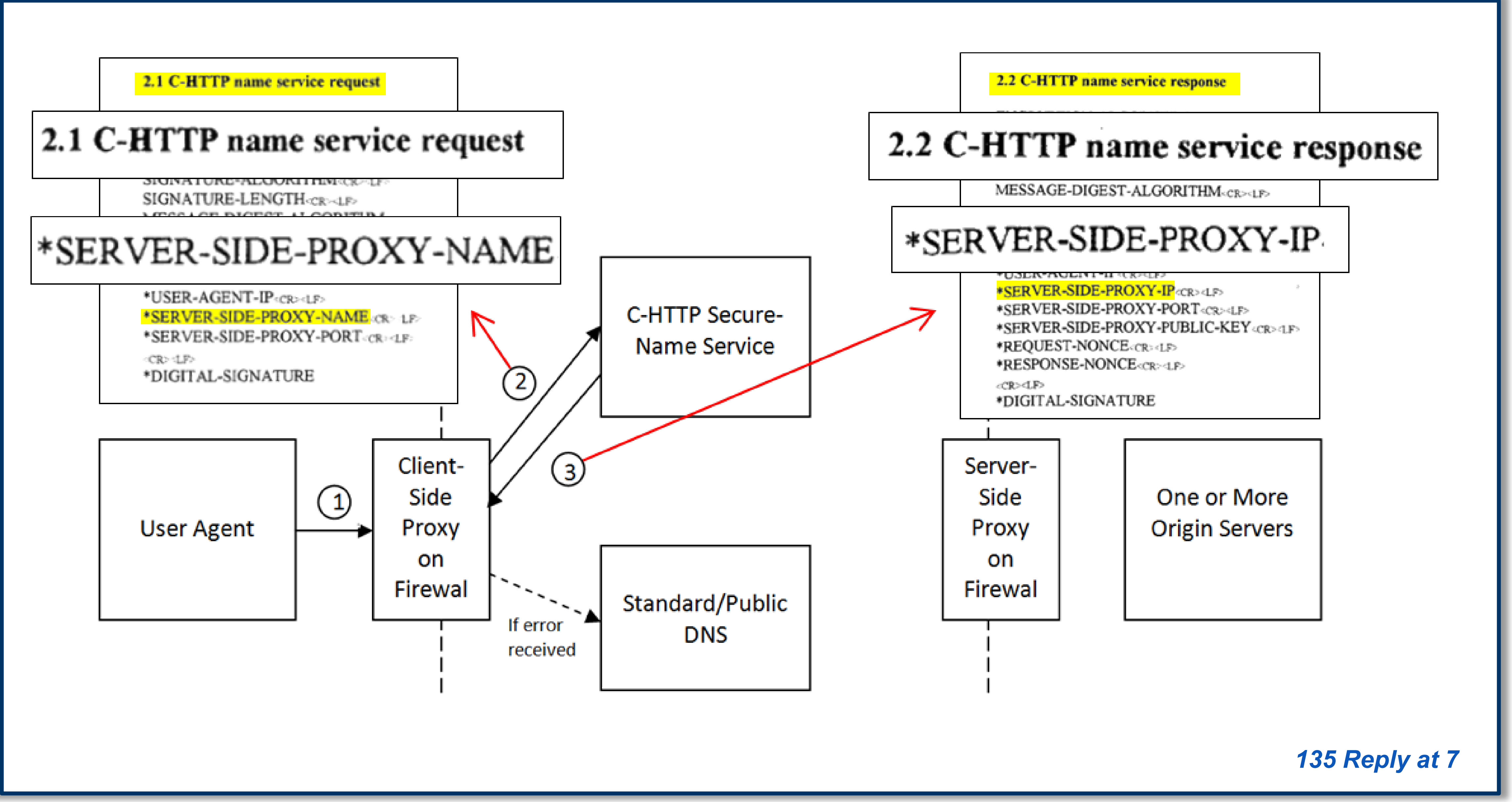
Kiuchi

“generating from the client computer a [DNS] request”

Kiuchi
Ex. 1002



C-HTTP -- The Development of a Secure, Closed HTTP-based Network
on the Internet



2.1 C-HTTP name service request

2.1 C-HTTP name service request

SIGNATURE-ALGORITHM<CR><LF>
SIGNATURE-LENGTH<CR><LF>
MESSAGE-DIGEST-ALGORITHM

***SERVER-SIDE-PROXY-NAME**

*USER-AGENT-IP<CR><LF>
*SERVER-SIDE-PROXY-NAME<CR><LF>
*SERVER-SIDE-PROXY-PORT<CR><LF>
<CR><LF>
*DIGITAL-SIGNATURE

2.2 C-HTTP name service response

2.2 C-HTTP name service response

MESSAGE-DIGEST-ALGORITHM<CR><LF>

***SERVER-SIDE-PROXY-IP**

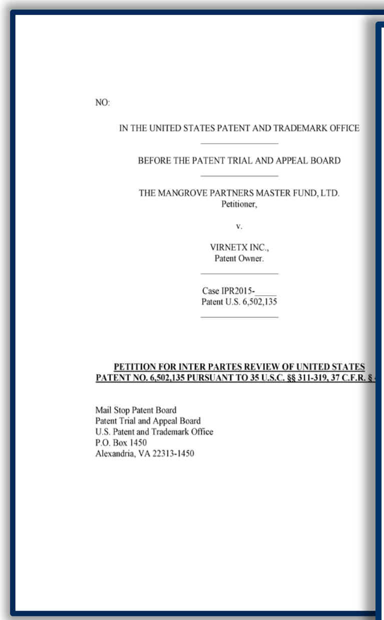
*USER-AGENT-IP<CR><LF>
*SERVER-SIDE-PROXY-IP<CR><LF>
*SERVER-SIDE-PROXY-PORT<CR><LF>
*SERVER-SIDE-PROXY-PUBLIC-KEY<CR><LF>
*REQUEST-NONCE<CR><LF>
*RESPONSE-NONCE<CR><LF>
<CR><LF>
*DIGITAL-SIGNATURE

135 Reply at 7

Kiuchi

“generating from the client computer a [DNS] request”

Petition
Paper 5



NO:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD.
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-_____
Patent U.S. 6,502,135

PETITION FOR INTER PARTES REVIEW OF UNITED STATES PATENT NO. 6,502,135 PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F.R. §

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Petition

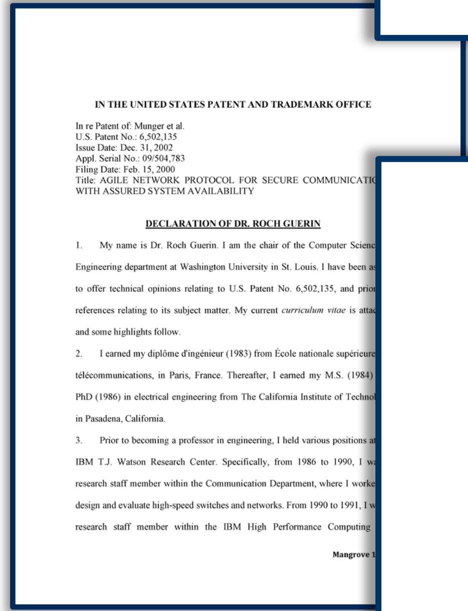
Kiuchi also discloses a process that includes “*generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer.*” *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 20-22. Kiuchi shows that a user agent makes an HTTP request to connect to a host that is specified within a URL. *See id.* The client-side proxy receives the request and sends a request to a C-HTTP name server asking to resolve the hostname in the request into an IP address. *See id.*

135 Pet. (Paper 5) at 27; see id. at 20-21

Kiuchi

“generating from the client computer a [DNS] request”

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIO
WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Scienc Engineering department at Washington University in St. Louis. I have been as to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior references relating to its subject matter. My current *curriculum vitae* is attac and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) PhD (1986) in electrical engineering from The California Institute of Technol in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I wa research staff member within the Communication Department, where I worke design and evaluate high-speed switches and networks. From 1990 to 1991, I w research staff member within the IBM High Performance Computing

Mangrove 1

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

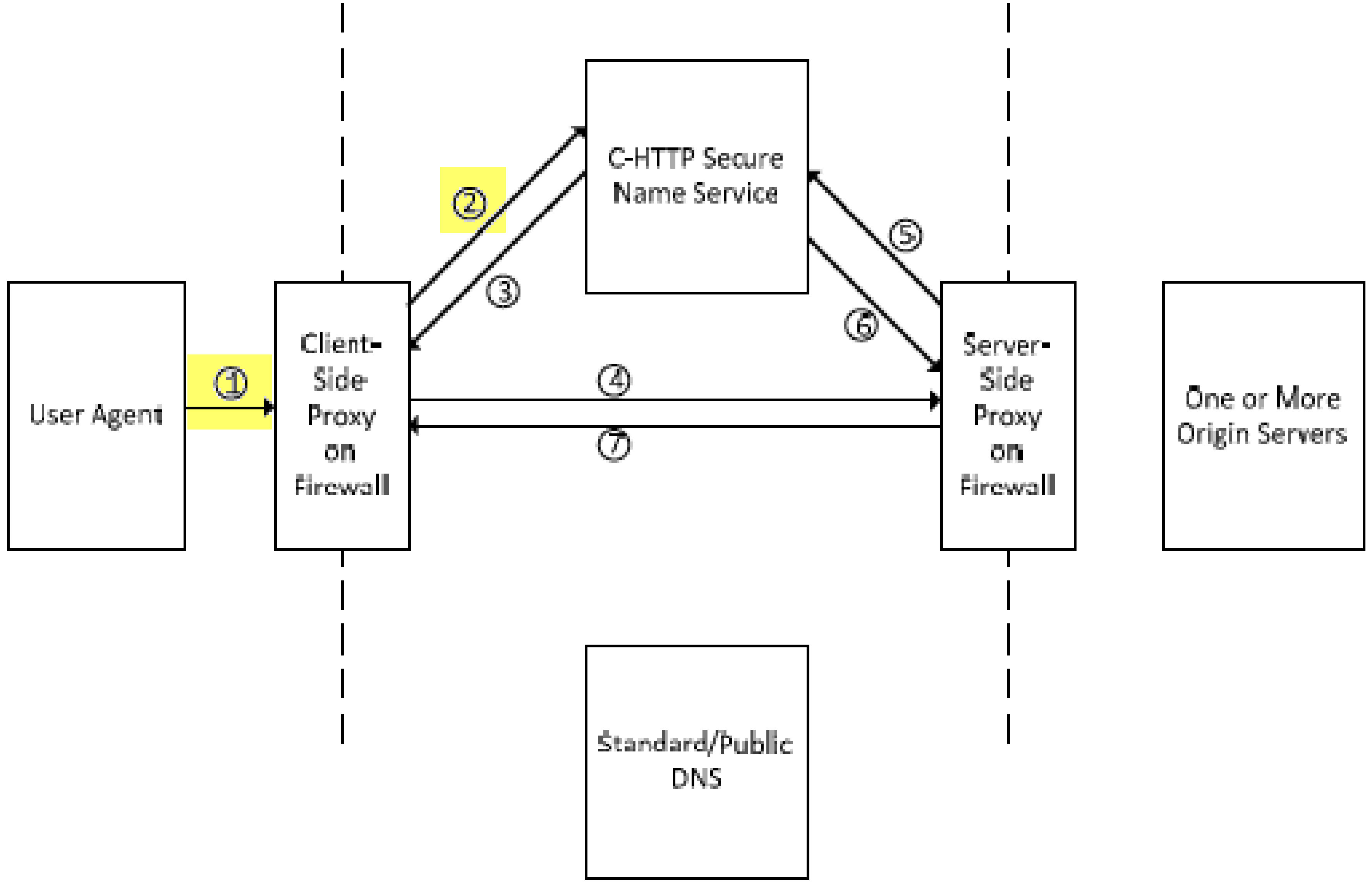
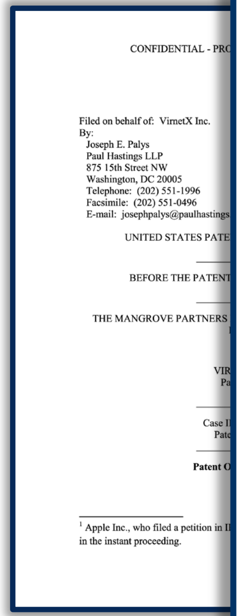

C-HTTP Secure Name Service
User Agent
①
②
③
Client-Side Proxy on Firewall
④
⑤
⑥
⑦
Server-Side Proxy on Firewall
One or More Origin Servers
Standard/Public DNS

Diagram 2

135 Pet. (Paper 5) at 20; Ex. 1003 at ¶20

VirnetX: C-HTTP Does Not Follow the DNS Protocol

Patent Owner's Res



CONFIDENTIAL - PRO

Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings

UNITED STATES PATE

BEFORE THE PATENT

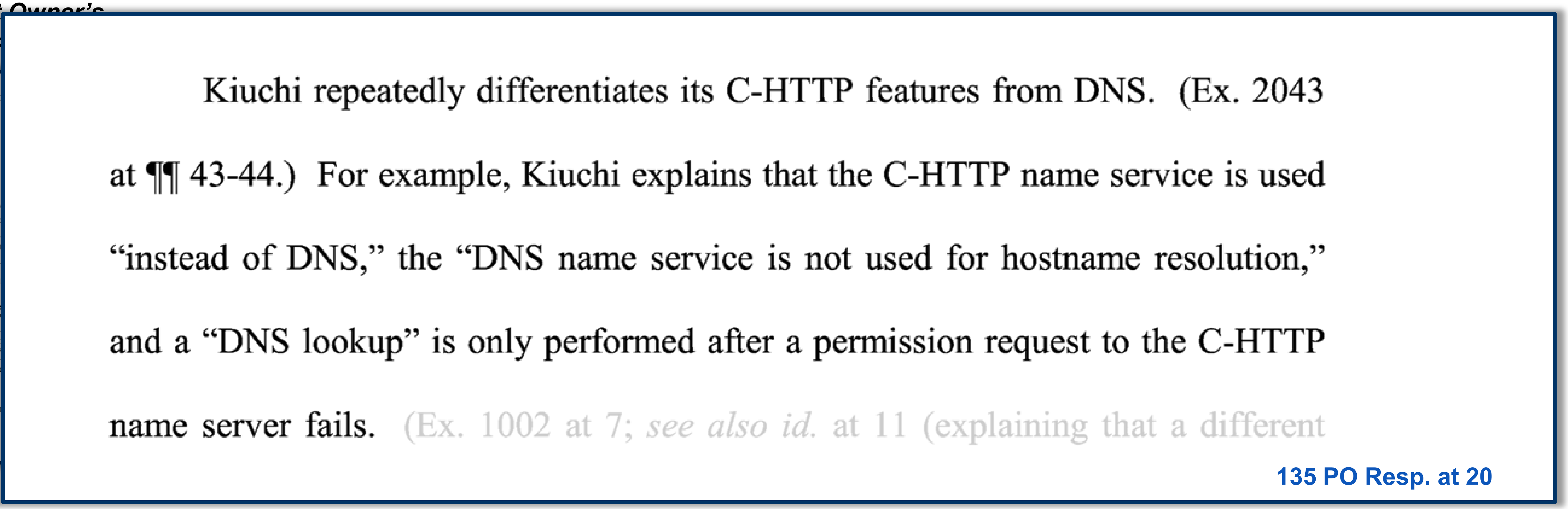
THE MANGROVE PARTNERS

VIR
Pa

Case I
Pate

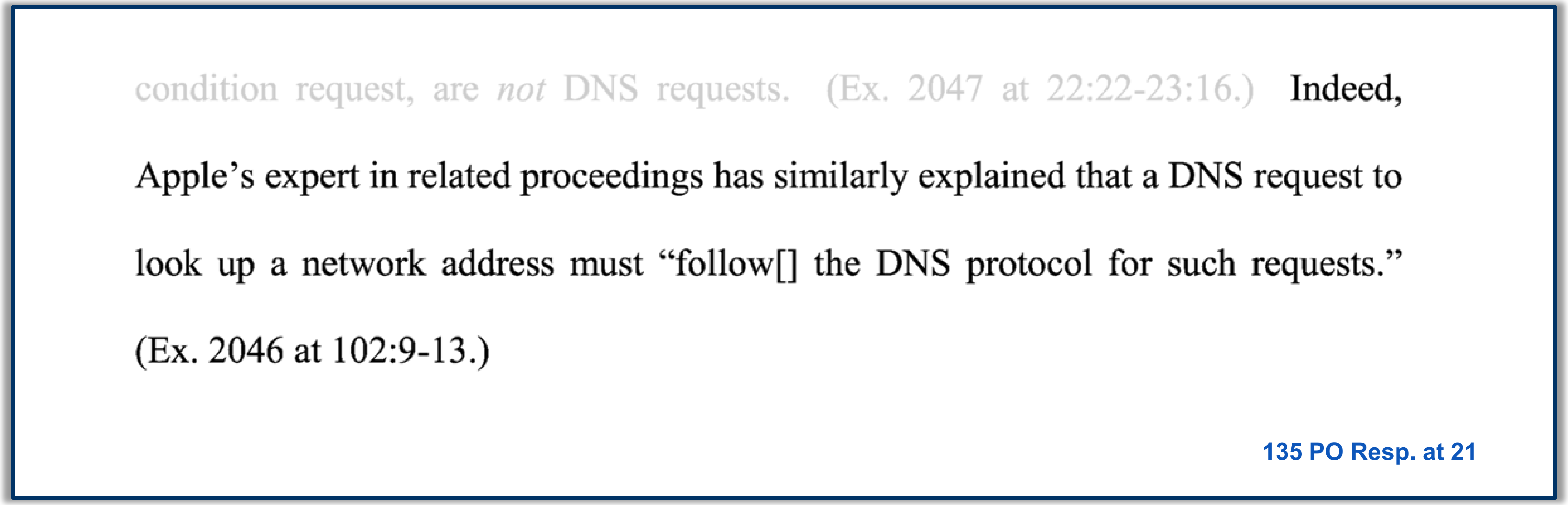
Patent O

[1] Apple Inc., who filed a petition in I
in the instant proceeding.



Kiuchi repeatedly differentiates its C-HTTP features from DNS. (Ex. 2043 at ¶¶ 43-44.) For example, Kiuchi explains that the C-HTTP name service is used "instead of DNS," the "DNS name service is not used for hostname resolution," and a "DNS lookup" is only performed after a permission request to the C-HTTP name server fails. (Ex. 1002 at 7; *see also id.* at 11 (explaining that a different

135 PO Resp. at 20



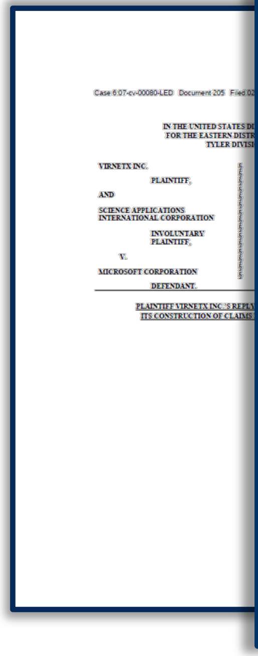
condition request, are *not* DNS requests. (Ex. 2047 at 22:22-23:16.) Indeed, Apple's expert in related proceedings has similarly explained that a DNS request to look up a network address must "follow[] the DNS protocol for such requests." (Ex. 2046 at 102:9-13.)

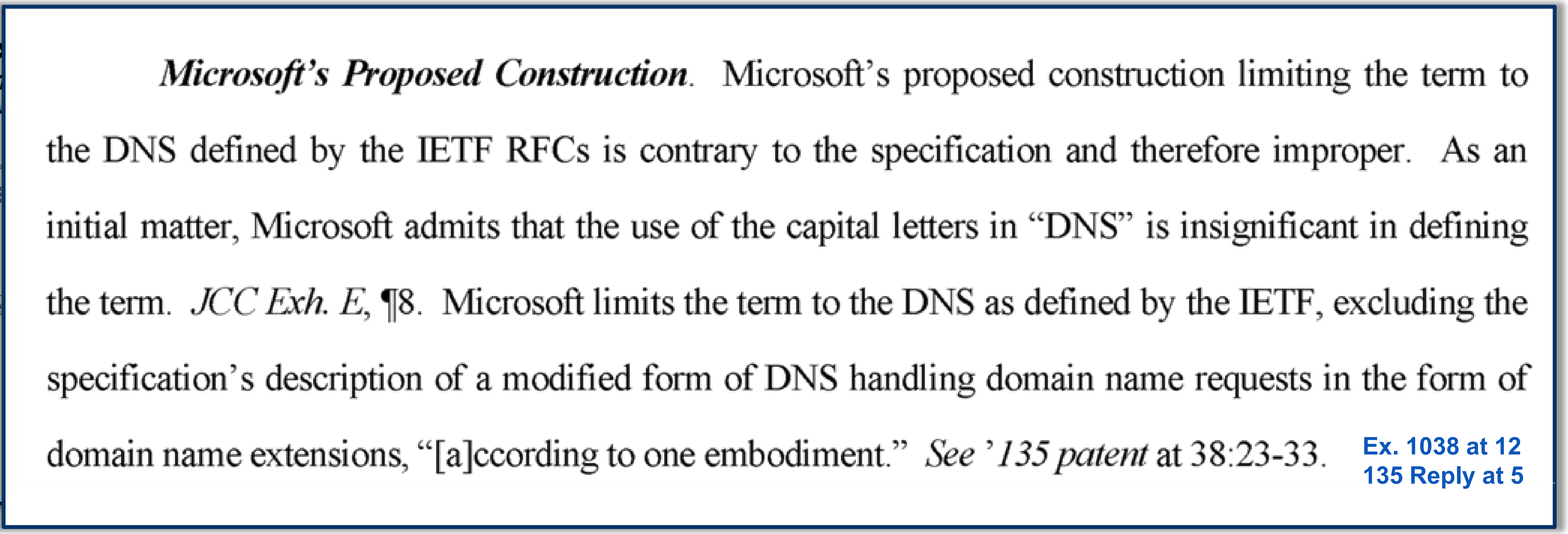
135 PO Resp. at 21

VirnetX: DNS Not Limited to the IETF DNS Protocol

Ex. 1038 (VirnetX's District Court Claim Construction Brief) & Ex. 1036 (Dr. Monrose)

VirnetX
Ex. 1

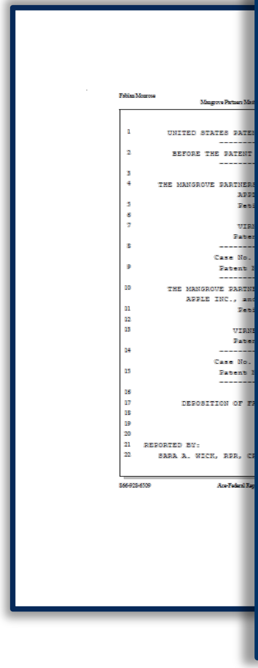


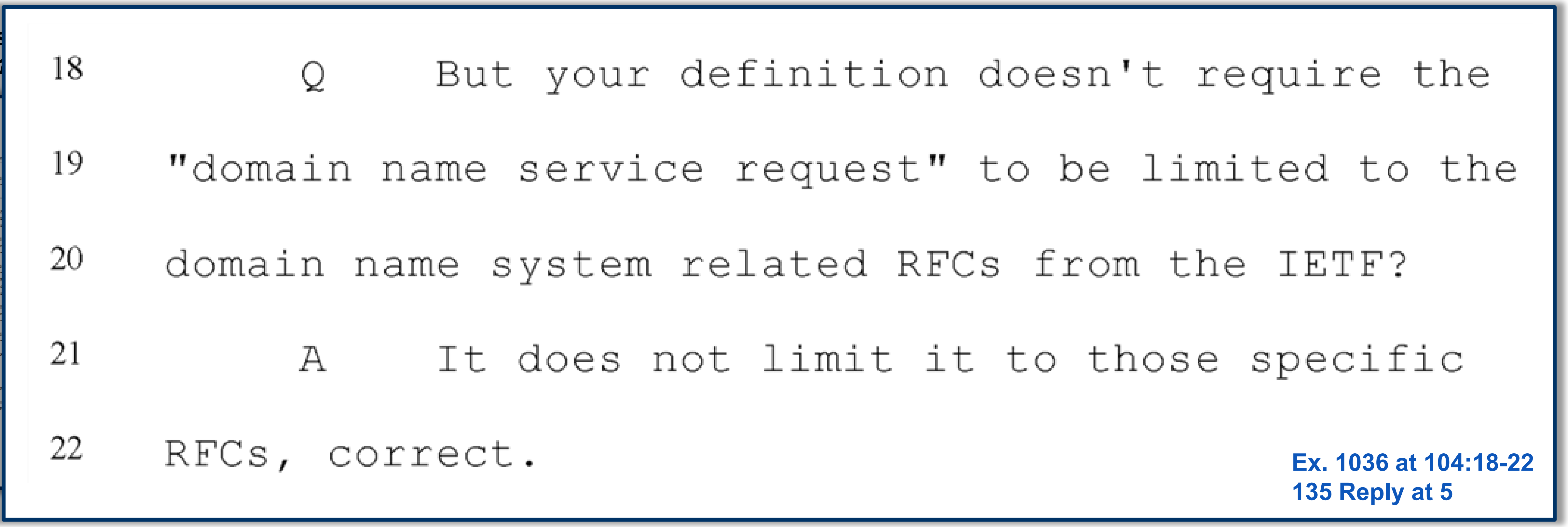


Microsoft's Proposed Construction. Microsoft's proposed construction limiting the term to the DNS defined by the IETF RFCs is contrary to the specification and therefore improper. As an initial matter, Microsoft admits that the use of the capital letters in "DNS" is insignificant in defining the term. *JCC Exh. E*, ¶8. Microsoft limits the term to the DNS as defined by the IETF, excluding the specification's description of a modified form of DNS handling domain name requests in the form of domain name extensions, "[a]ccording to one embodiment." *See '135 patent* at 38:23-33.

Ex. 1038 at 12
135 Reply at 5

Monros
Ex. 1



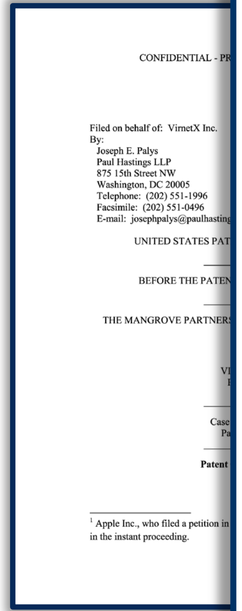


```
        Q     But your definition doesn't require the
"domain name service request" to be limited to the
domain name system related RFCs from the IETF?
        A     It does not limit it to those specific
RFCs, correct.
```

Ex. 1036 at 104:18-22
135 Reply at 5

VirnetX: C-HTTP Name Server Does Not Return the Address "Corresponding" to the Domain Name

Patent
Res



CONFIDENTIAL - PR

Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhasting

UNITED STATES PAT

BEFORE THE PATEN

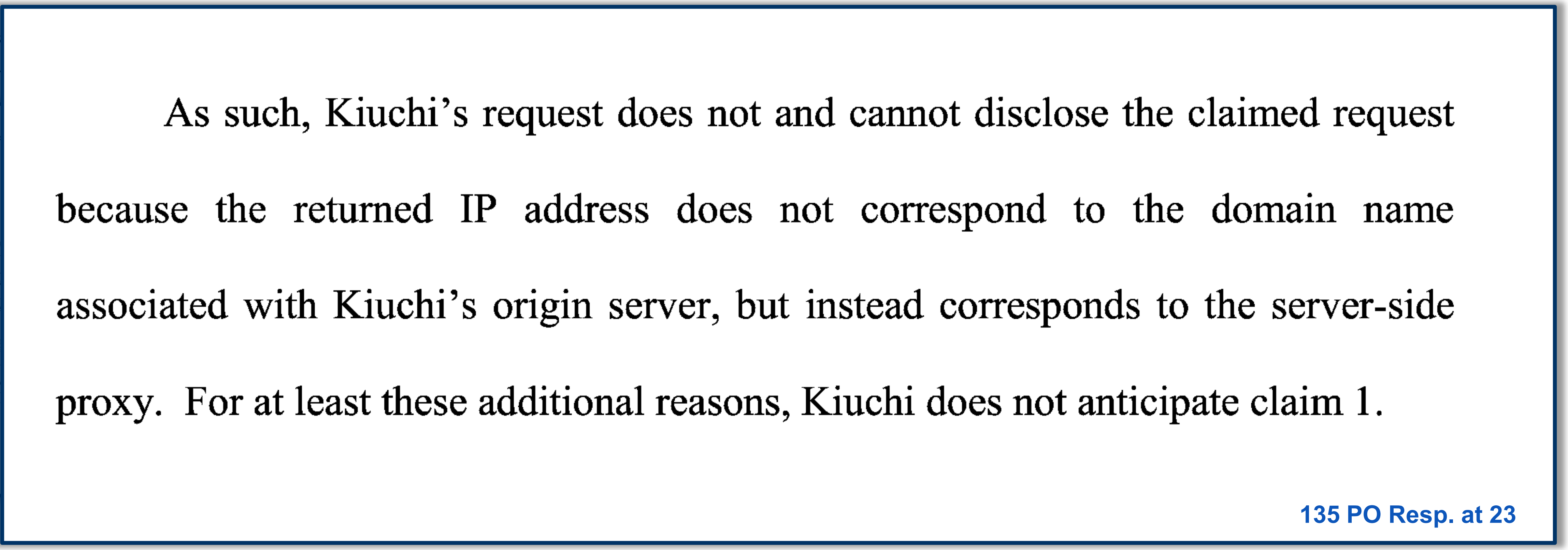
THE MANGROVE PARTNERS

VI
I

Case
Pa

Patent

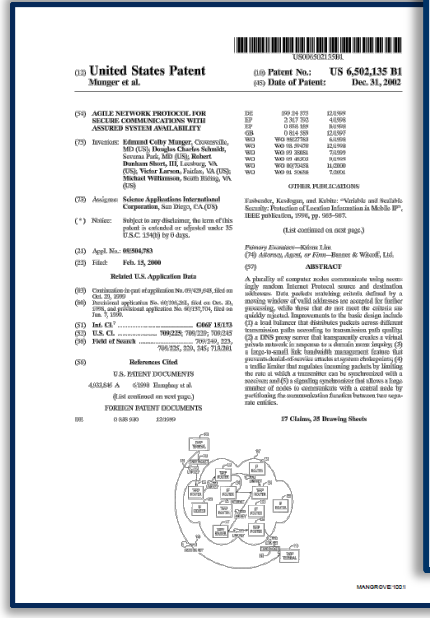
[1] Apple Inc., who filed a petition in
in the instant proceeding.



As such, Kiuchi's request does not and cannot disclose the claimed request because the returned IP address does not correspond to the domain name associated with Kiuchi's origin server, but instead corresponds to the server-side proxy. For at least these additional reasons, Kiuchi does not anticipate claim 1.

135 PO Resp. at 23

135 Patent
Ex. 1001



US006502135B1

(12) United States Patent
Munger et al.

(10) Patent No.: US 6,502,135 B1
(45) Date of Patent: Dec. 31, 2002

(54) AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

(75) Inventors: Edmund Colby Munger, Crownsville, MD (US); Douglas Charles Schmidt, Severna Park, MD (US); Robert Dunham Short, III, Leesburg, VA (US); Victor Larson, Fairfax, VA (US); Michael Williamson, South Riding, VA (US)

(73) Assignee: Science Applications International Corporation, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/504,783

(22) Filed: Feb. 15, 2000

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) Int. Cl.^{7} G06F 15/173
(52) U.S. Cl. 709/225; 709/229; 709/245
(58) Field of Search 709/249, 223, 709/225, 229, 245; 713/201

(56) References Cited

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication, 1996, pp. 963–967.

(List continued on next page.)

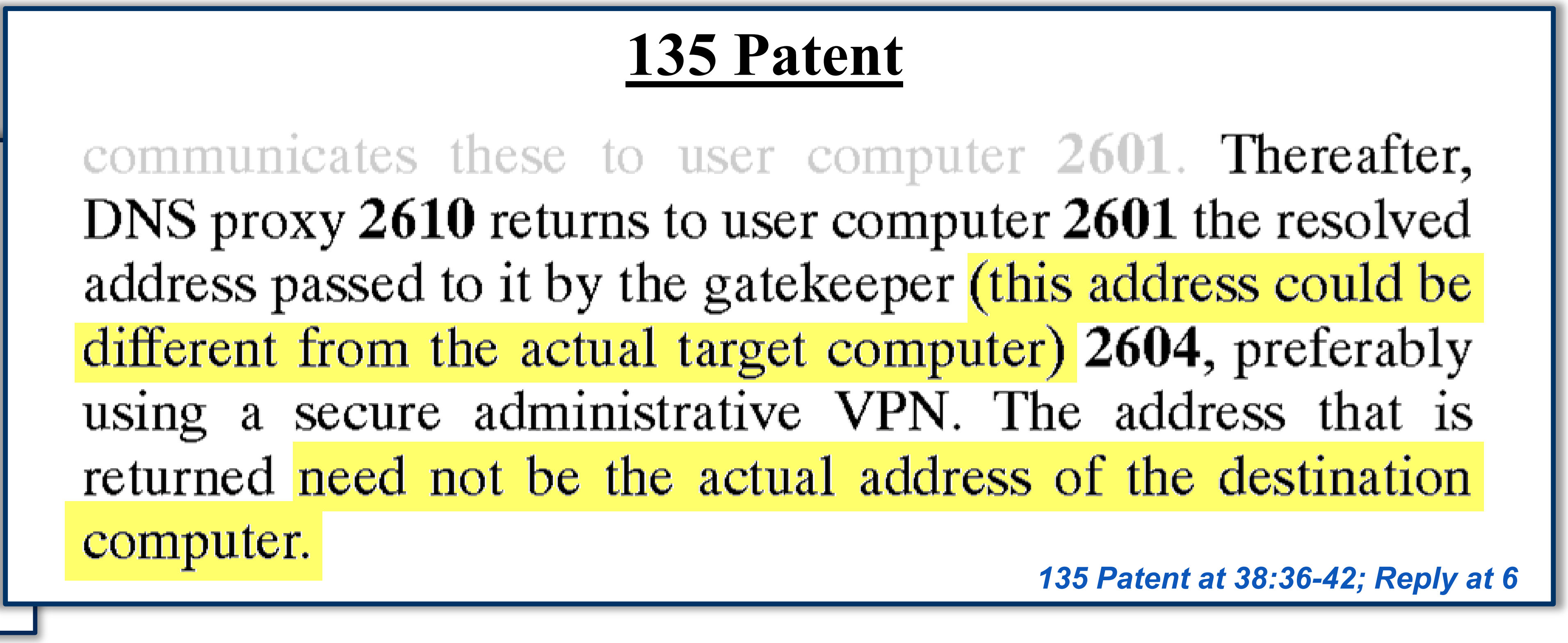
Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(57) ABSTRACT

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design 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.

17 Claims, 35 Drawing Sheets

MANGROVE 1001



135 Patent

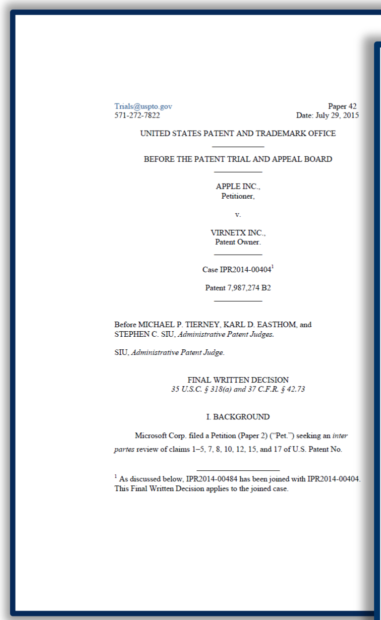
communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

135 Patent at 38:36-42; Reply at 6

IPR2014-00404: Kiuchi's Server-Side Proxy Is the "Host"

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404
Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

SIU, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Microsoft Corp. filed a Petition (Paper 2) ("Pet.") seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

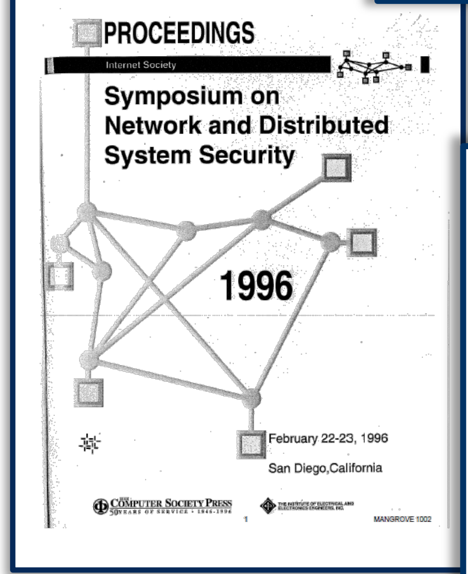
[1] As discussed below, IPR2014-00484 has been joined with IPR2014-00404. This Final Written Decision applies to the joined case.

Patent Owner argues that Kiuchi discloses that the client-side proxy sends a request for a network address for the "origin server" but not for the server-side proxy. However, Kiuchi discloses that in response to the request to communicate with "the host," the name server examines "the requested *server-side proxy*" and returns "the IP address . . . of the *server-side proxy*." Ex. 1004, 65 (emphasis added). Thus, contrary to Patent Owner's contention, "the host" of Kiuchi corresponds to the "server-side proxy" (or second network device, as recited in claim 1).

Final Written Decision (Paper 42) at 11-12; 135 Reply at 7; 151 Reply at 6

Kiuchi: the Host Is the Server-Side Proxy

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

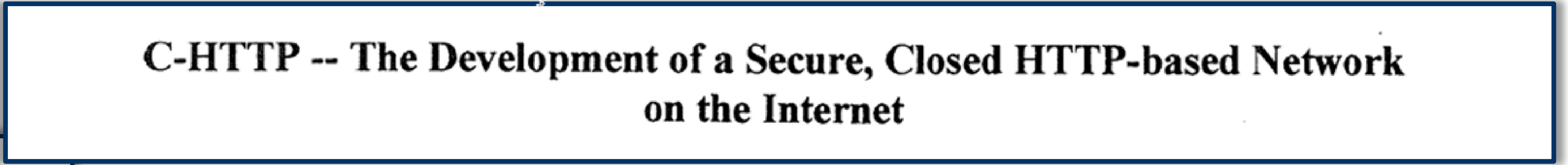
Symposium on
Network and Distributed
System Security

1996

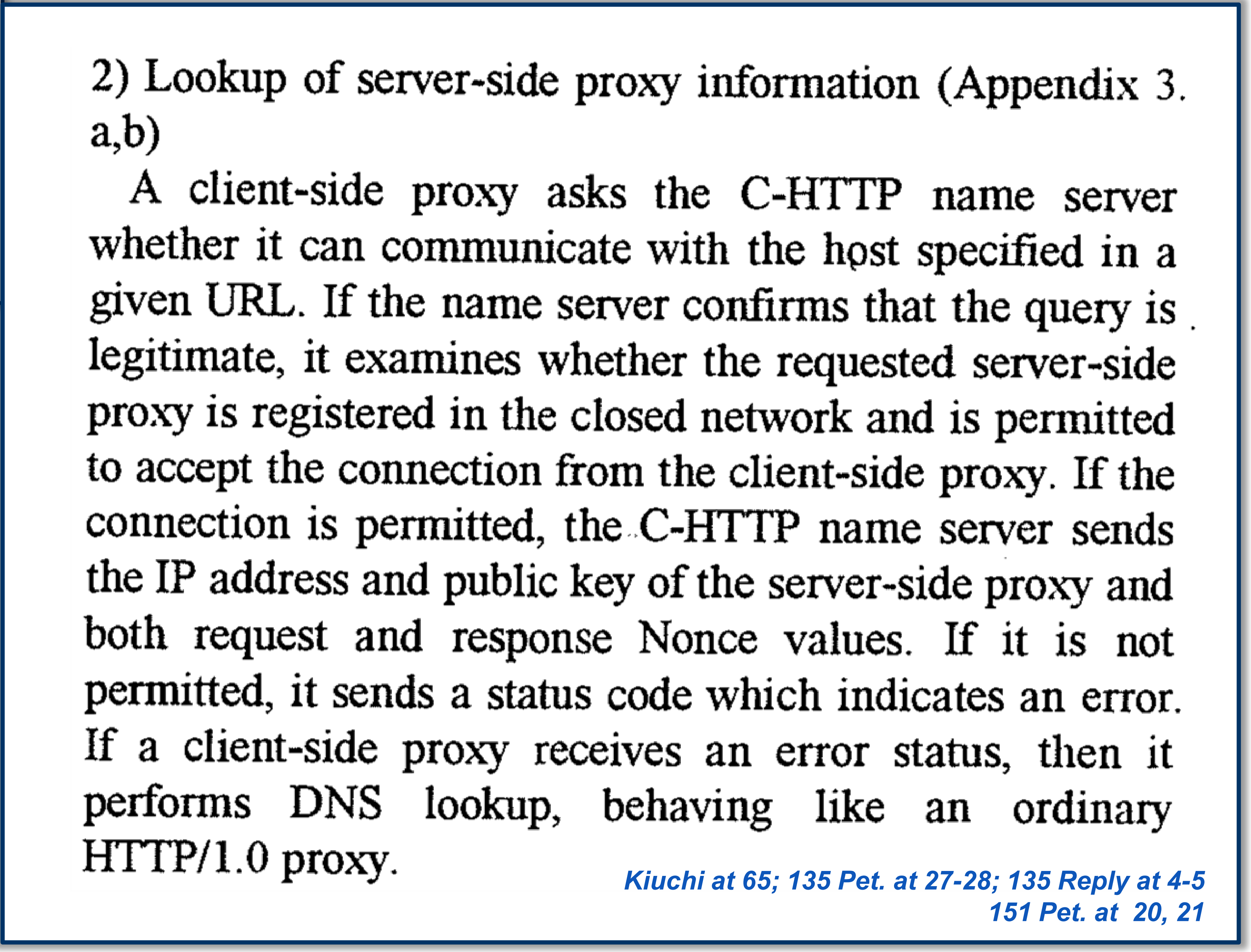
February 22-23, 1996
San Diego,California

COMPUTER SOCIETY PRESS

MANGROVE 1002



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



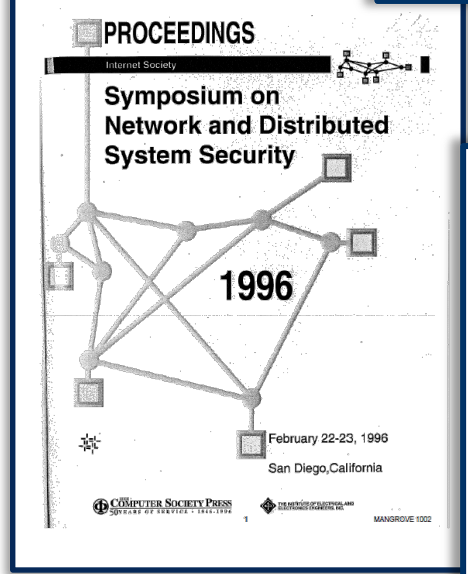
2) Lookup of server-side proxy information (Appendix 3. a,b)

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. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.

Kiuchi at 65; 135 Pet. at 27-28; 135 Reply at 4-5
151 Pet. at 20, 21

Kiuchi: the Host Is the Server-Side Proxy

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

Symposium on
Network and Distributed
System Security

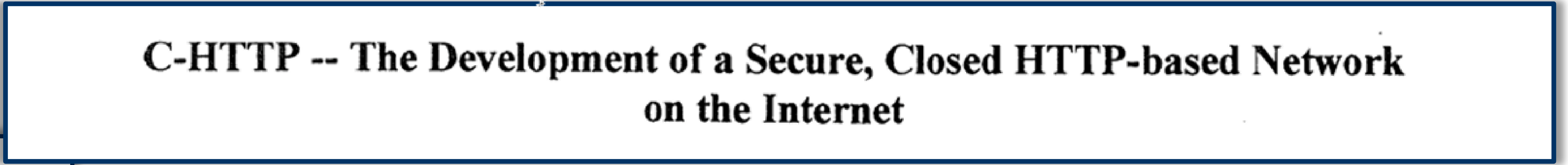
1996

February 22-23, 1996

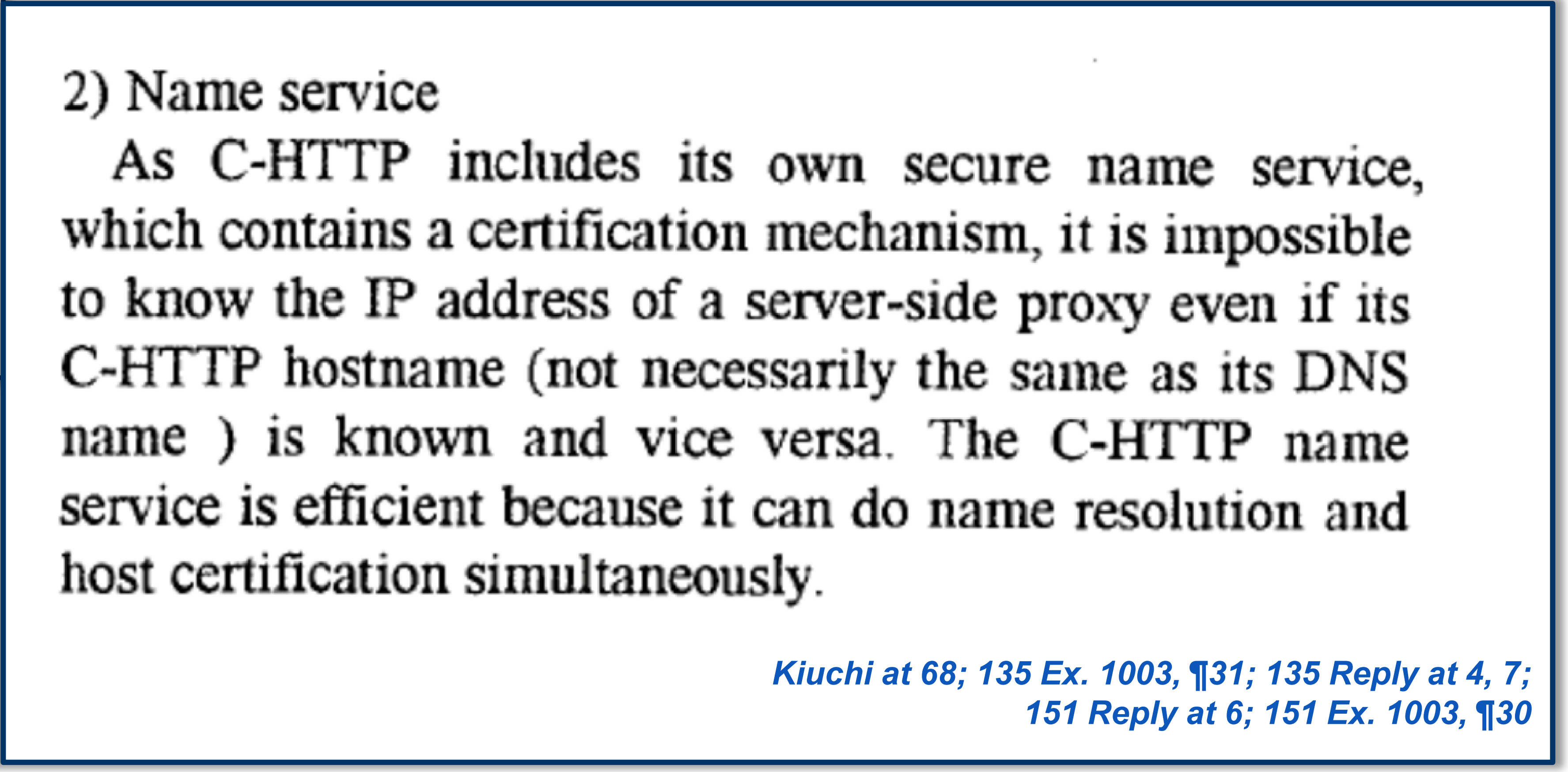
San Diego,California

COMPUTER SOCIETY PRESS

MANGROVE 1002



C-HTTP -- The Development of a Secure, Closed HTTP-based Network
on the Internet



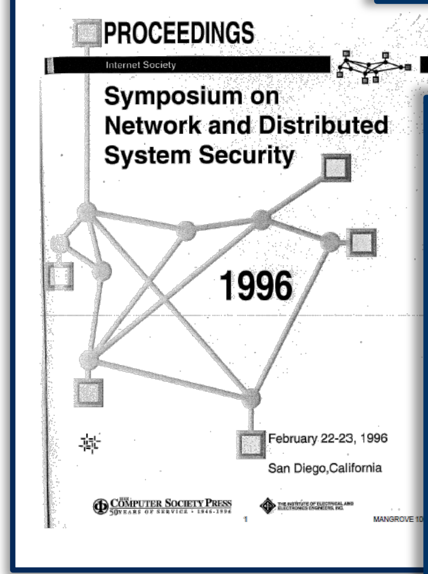
2) Name service

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. The C-HTTP name service is efficient because it can do name resolution and host certification simultaneously.

Kiuchi at 68; 135 Ex. 1003, ¶31; 135 Reply at 4, 7;
151 Reply at 6; 151 Ex. 1003, ¶30

Kiuchi: the Host Is the Server-Side Proxy

Kiuchi
Ex. 1002



PROCEEDINGS

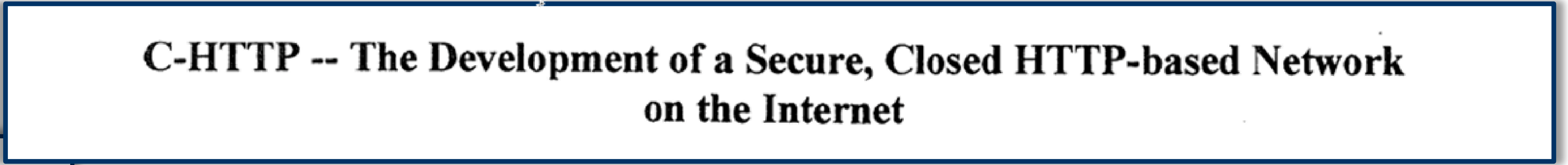
Internet Society

Symposium on
Network and Distributed
System Security

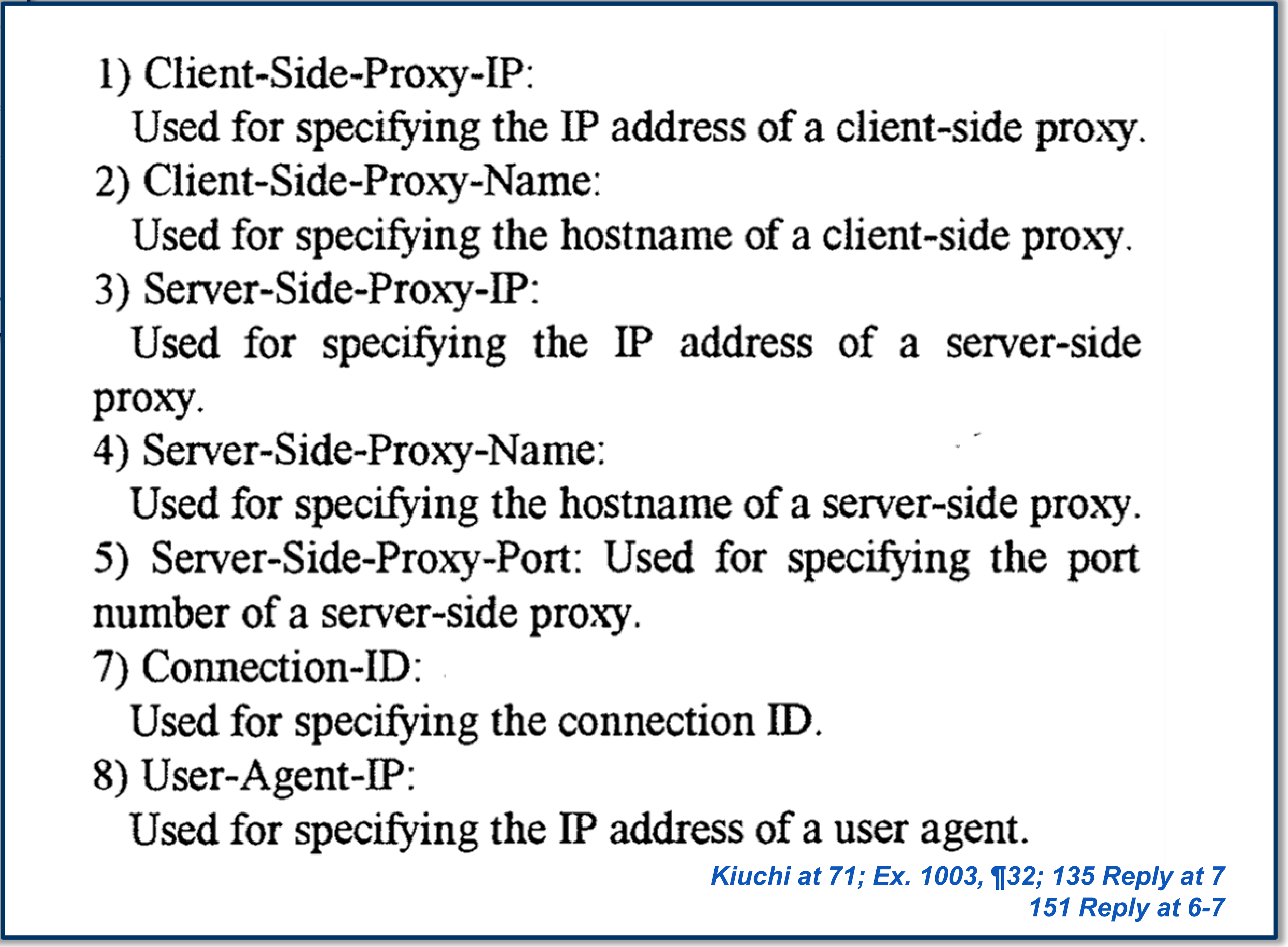
1996

February 22-23, 1996
San Diego,California

COMPUTER SOCIETY PRESS



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



1) Client-Side-Proxy-IP:
Used for specifying the IP address of a client-side proxy.

2) Client-Side-Proxy-Name:
Used for specifying the hostname of a client-side proxy.

3) Server-Side-Proxy-IP:
Used for specifying the IP address of a server-side proxy.

4) Server-Side-Proxy-Name:
Used for specifying the hostname of a server-side proxy.

5) Server-Side-Proxy-Port: Used for specifying the port number of a server-side proxy.

7) Connection-ID:
Used for specifying the connection ID.

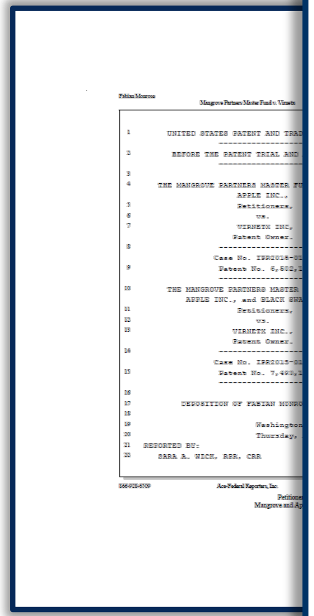
8) User-Agent-IP:
Used for specifying the IP address of a user agent.

Kiuchi at 71; Ex. 1003, ¶32; 135 Reply at 7
151 Reply at 6-7

Dr. Monrose Considered Materials Not of Record

Ex. 1036 – Deposition Transcript of Dr. Fabian Monrose (April 28, 2016)

Monrose I
Ex. 103



Fabian Monrose
Mangrove Partners Master Fund v. Virnetx

UNITED STATES PATENT AND TRAD
BEFORE THE PATENT TRIAL AND
THE MANGROVE PARTNERS MASTER FU
APPLE INC.,
Petitioners,
vs.
VIRNETX INC,
Patent Owner.
Case No. IPR2015-01
Patent No. 6,502,1
THE MANGROVE PARTNERS MASTER
APPLE INC., and BLACK SWA
Petitioners,
vs.
VIRNETX INC.,
Patent Owner.
Case No. IPR2015-01
Patent No. 7,490,1
DEPOSITION OF FABIAN MONRO
Washington
Thursday,
REPORTED BY:
SARA A. WICK, RPR, CRR

866-928-6509 Ace-Federal Reporters, Inc.
Petitione
Mangrove and Ap

THE WITNESS: Like I said, I see the mapping. Sitting here today, I don't remember the specifics offhand, but I remember in a previous evaluation I looked, there was a correction submitted -- I don't remember the exhibit number -- that talked about a presentation which corrected some of these. And so I would have to look back at that to --

Ex. 1036 at 172:13-20
135 Reply at 8
151 Reply at 7

Q And you've mentioned that correction a few times. You didn't mention that correction in your declaration, did you?

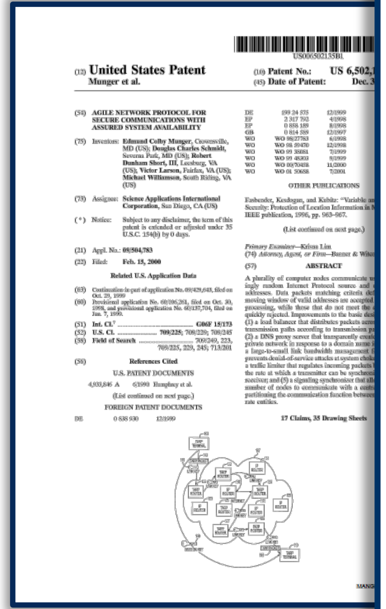
A I did not. I don't think it was an exhibit in these at that time.

Ex. 1036 at 205:18-22
135 Reply at 8
151 Reply at 7

135 Patent: Step 2

"determining whether… access to a secure web site [was requested]"

135 Patent
Ex. 1001



US006502135B1

(12) United States Patent
Munger et al.

(10) Patent No.: US 6,502,1
(45) Date of Patent: Dec. 3

(54) AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

(75) Inventors: Edmund Colby Munger, Crownsville, MD (US); Douglas Charles Schmidt, Severna Park, MD (US); Robert Dunham Short, III, Leesburg, VA (US); Victor Larson, Fairfax, VA (US); Michael Williamson, South Riding, VA (US)

(73) Assignee: Science Applications International Corporation, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/504,783

(22) Filed: Feb. 15, 2000

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) Int. Cl.^{7} G06F 15/173

(52) U.S. Cl. 709/225; 709/229; 709/245

(58) Field of Search 709/249, 223, 709/225, 229, 245; 713/201

(56) References Cited

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable an Security: Protection of Location Information in M IEEE publication, 1996, pp. 963–967.

(List continued on next page.)

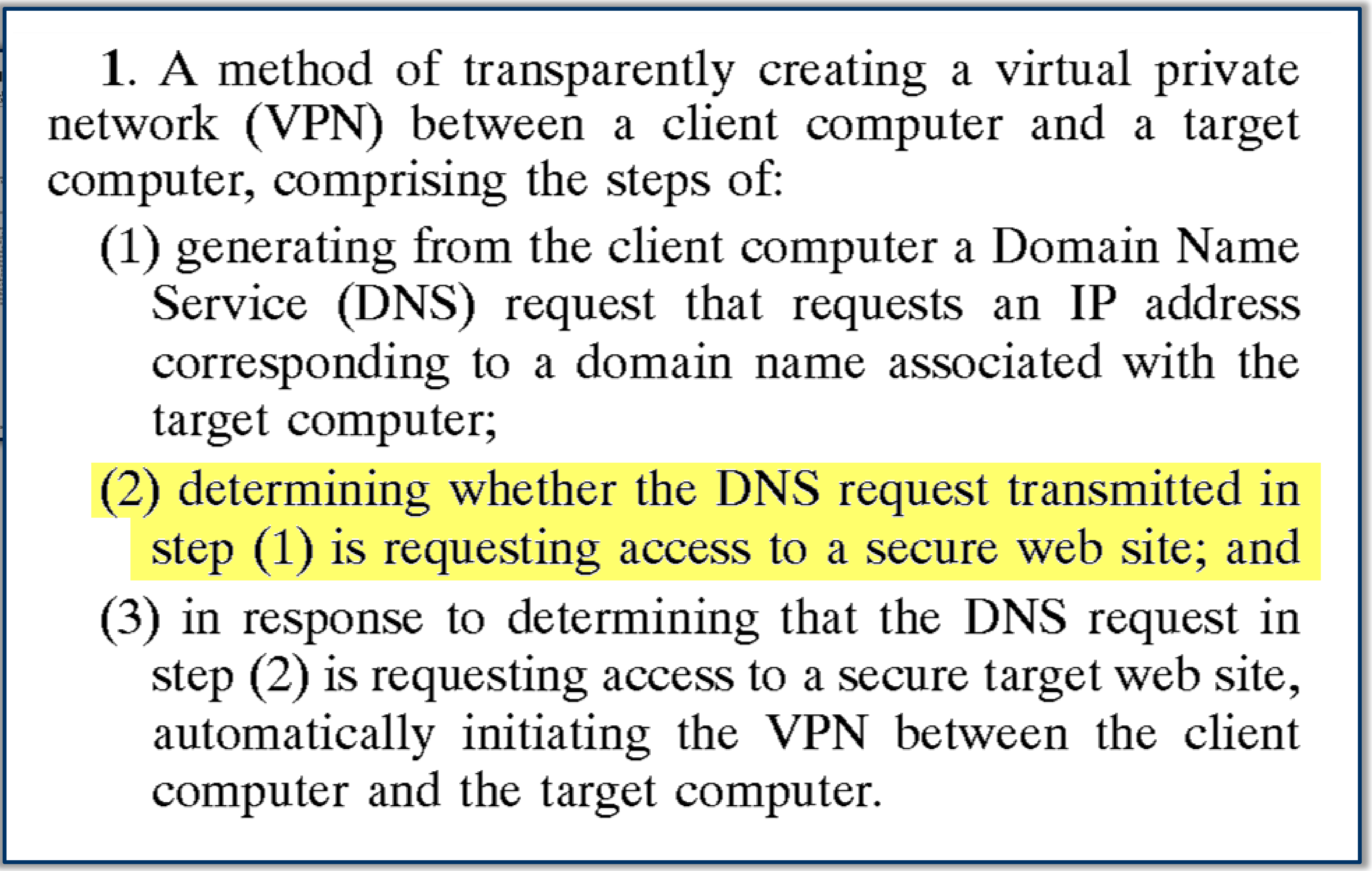
Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witco

(57) ABSTRACT

A plurality of computer nodes communicate us ingly random Internet Protocol source and d addresses. Data packets matching criteria def moving window of valid addresses are accepted processing, while those that do not meet the c quickly rejected. Improvements to the basic desi (1) a load balancer that distributes packets acros transmission paths according to transmission pa (2) a DNS proxy server that transparently creat private network in response to a domain name i a large-to-small link bandwidth management f prevents denial-of-service attacks at system choke a traffic limiter that regulates incoming packets b the rate at which a transmitter can be synchroni receiver; and (5) a signaling synchronizer that allo number of nodes to communicate with a centra partitioning the communication function betwee rate entities.

17 Claims, 35 Drawing Sheets

MANG



1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

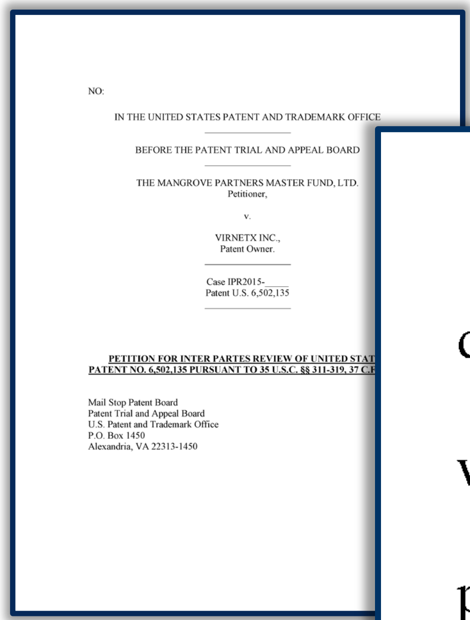
(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

Kiuchi

“determining whether… access to a secure web site [was requested]”

Petition
Paper 5



NO:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD.
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-_____
Patent U.S. 6,502,135

PETITION FOR INTER PARTES REVIEW OF UNITED STAT
PATENT NO. 6,502,135 PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Petition

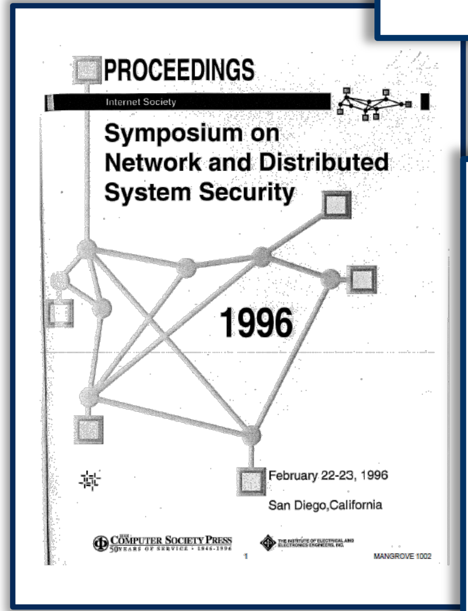
If the C-HTTP name server determines the hostname specifies a secure destination and the connection is permitted, it will return an IP address associated with the secure hostname along with other information. *See id.* The client-side proxy uses the returned IP address to send a request to the server-side proxy to make a connection. *See id.* Thus, the C-HTTP name server and client-side proxy each determine whether the user agent is requesting to connect to a secure destination. *See* Ex. 1003, ¶¶ 23-24.

135 Pet. (Paper 5) at 28

Kiuchi

“determining whether… access to a secure web site [was requested]”

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

Symposium on
Network and Distributed
System Security

1996

February 22-23, 1996
San Diego,California

COMPUTER SOCIETY PRESS

MANGROVE 1002

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

2) Lookup of server-side proxy information (Appendix 3. a,b)

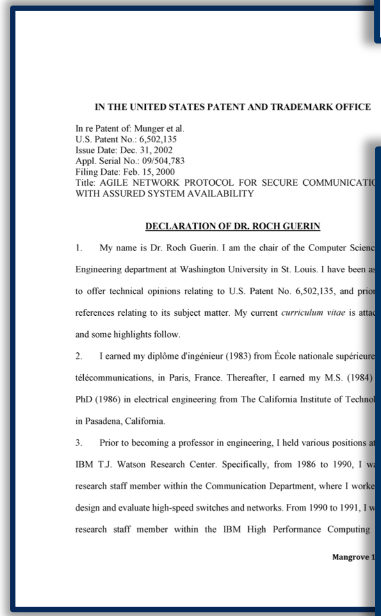
A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection 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. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.

Kiuchi at 65; 135 Pet. at 27-28

Kiuchi

“determining whether… access to a secure web site [was requested]”

Dr. Guerin Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIC
WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Scienc Engineering department at Washington University in St. Louis. I have been as to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior references relating to its subject matter. My current *curriculum vitae* is attac and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) PhD (1986) in electrical engineering from The California Institute of Technol in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I wa research staff member within the Communication Department, where I worke design and evaluate high-speed switches and networks. From 1990 to 1991, I w research staff member within the IBM High Performance Computing

Mangrove 1

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

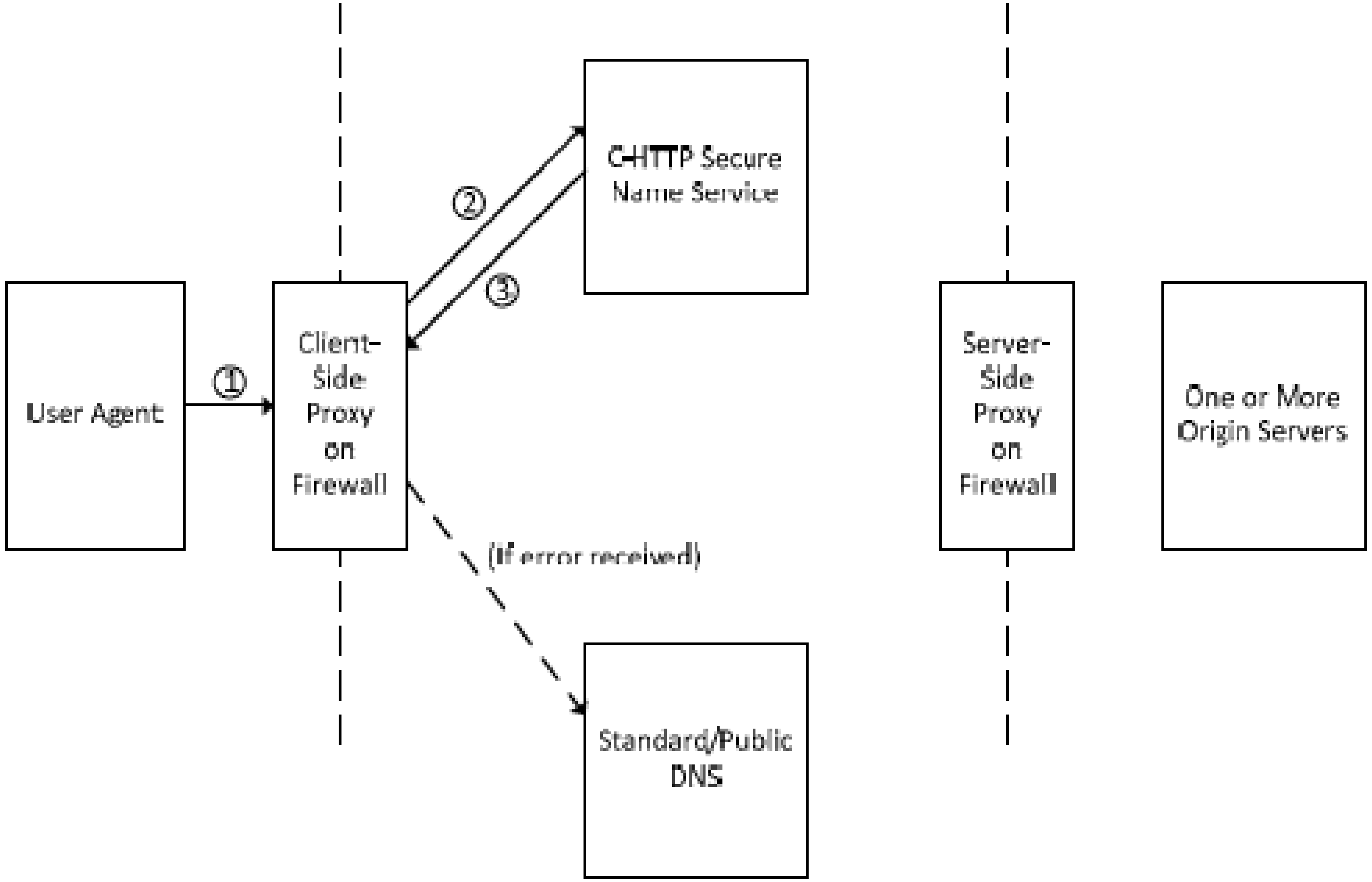

C-HTTP Secure Name Service
②
③
User Agent
①
Client-Side Proxy on Firewall
(If error received)
Standard/Public DNS
Server-Side Proxy on Firewall
One or More Origin Servers

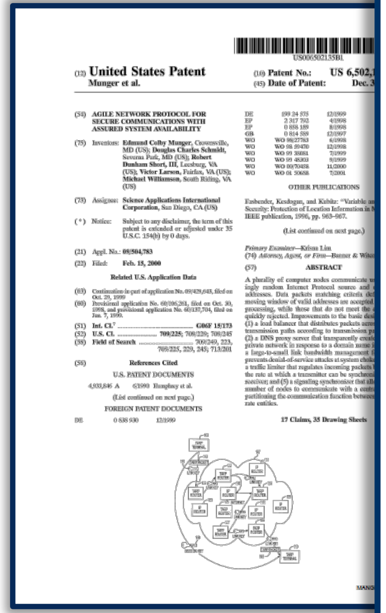
Diagram 3

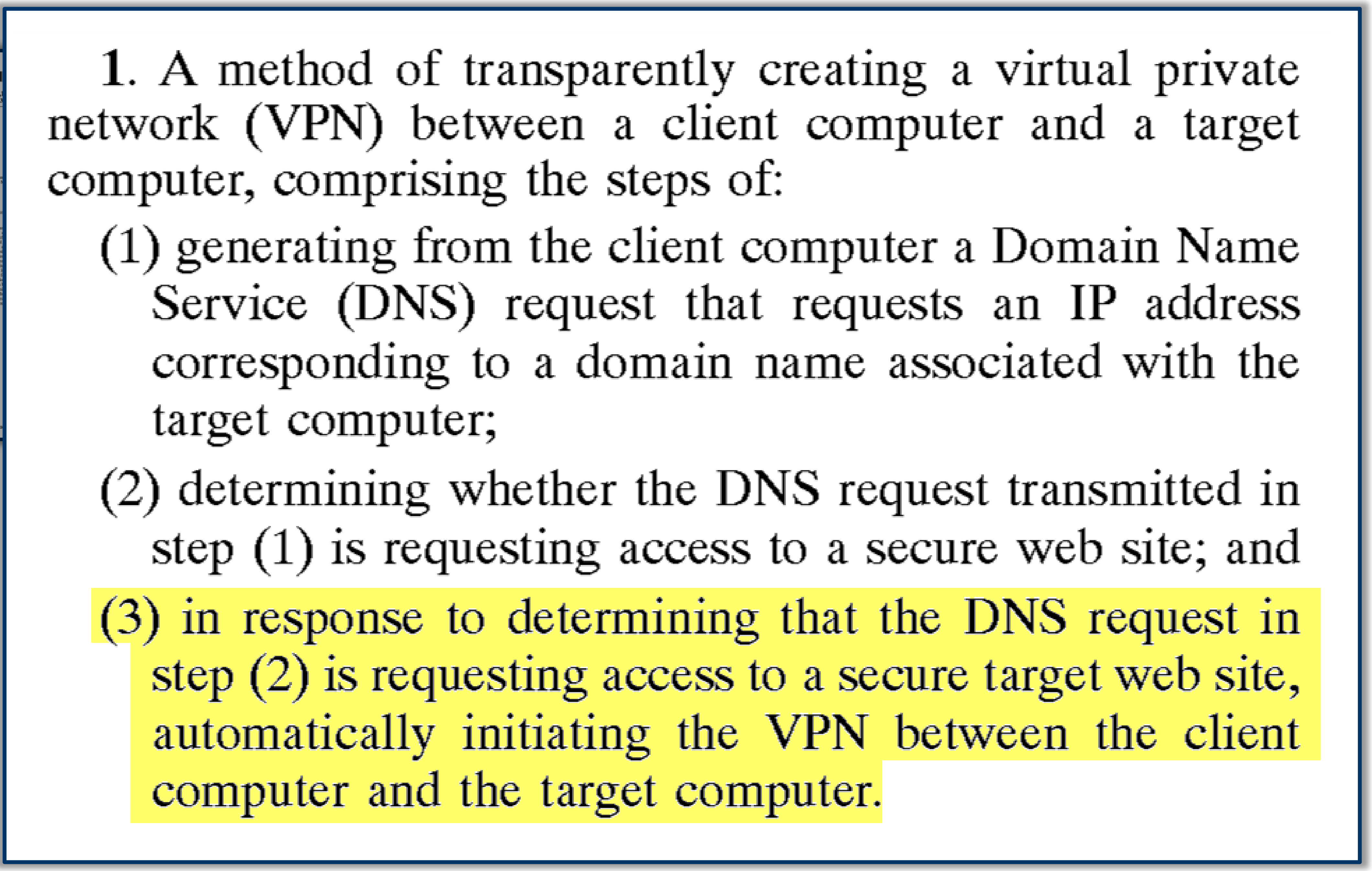
135 Pet. (Paper 5) at 21

135 Patent: Step 3

"in response… automatically initiating the VPN"

135 Patent
Ex. 1001





1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

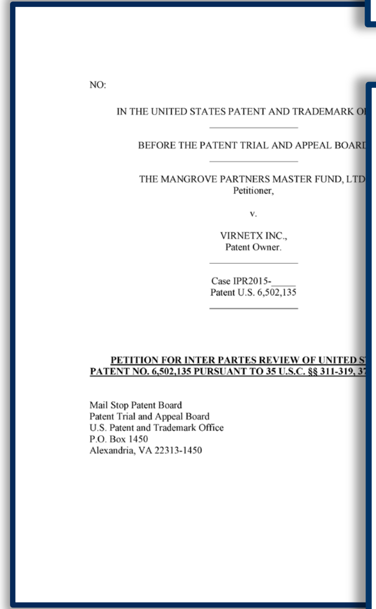
(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

Kiuchi

"in response… automatically initiating the VPN"

Petition Paper 5



NO:

IN THE UNITED STATES PATENT AND TRADEMARK O

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-_____
Patent U.S. 6,502,135

PETITION FOR INTER PARTES REVIEW OF UNITED S
PATENT NO. 6,502,135 PURSUANT TO 35 U.S.C. §§ 311-319, 37

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Petition

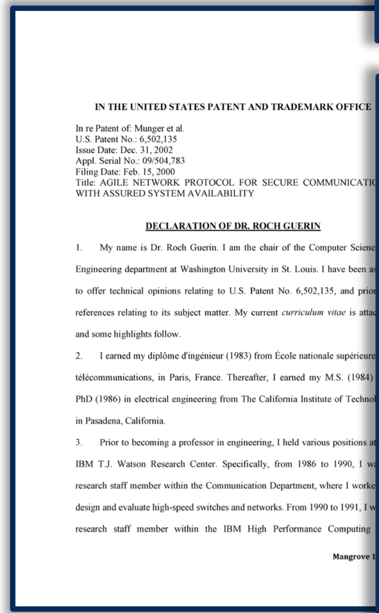
sent between them. *See* Ex. 1002, p. 65, § 1; *see also* Ex. 1003, ¶ 26. The connect message the client-side proxy sends to the server-side proxy and the response message the server-side proxy sends to the client- side proxy (both of which are sent without intervention from the user agent) act to initiate the connection. *See* Ex. 1002, pp. 65-66, § 2.3; *see also* Ex. 1003, ¶¶ 27-30.

135 Pet. at 29

Kiuchi

"in response… automatically initiating the VPN"

Dr. Guerin Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIC
WITH ASSURED SYSTEM AVAILABILITY

DECLARATION OF DR. ROCH GUERIN

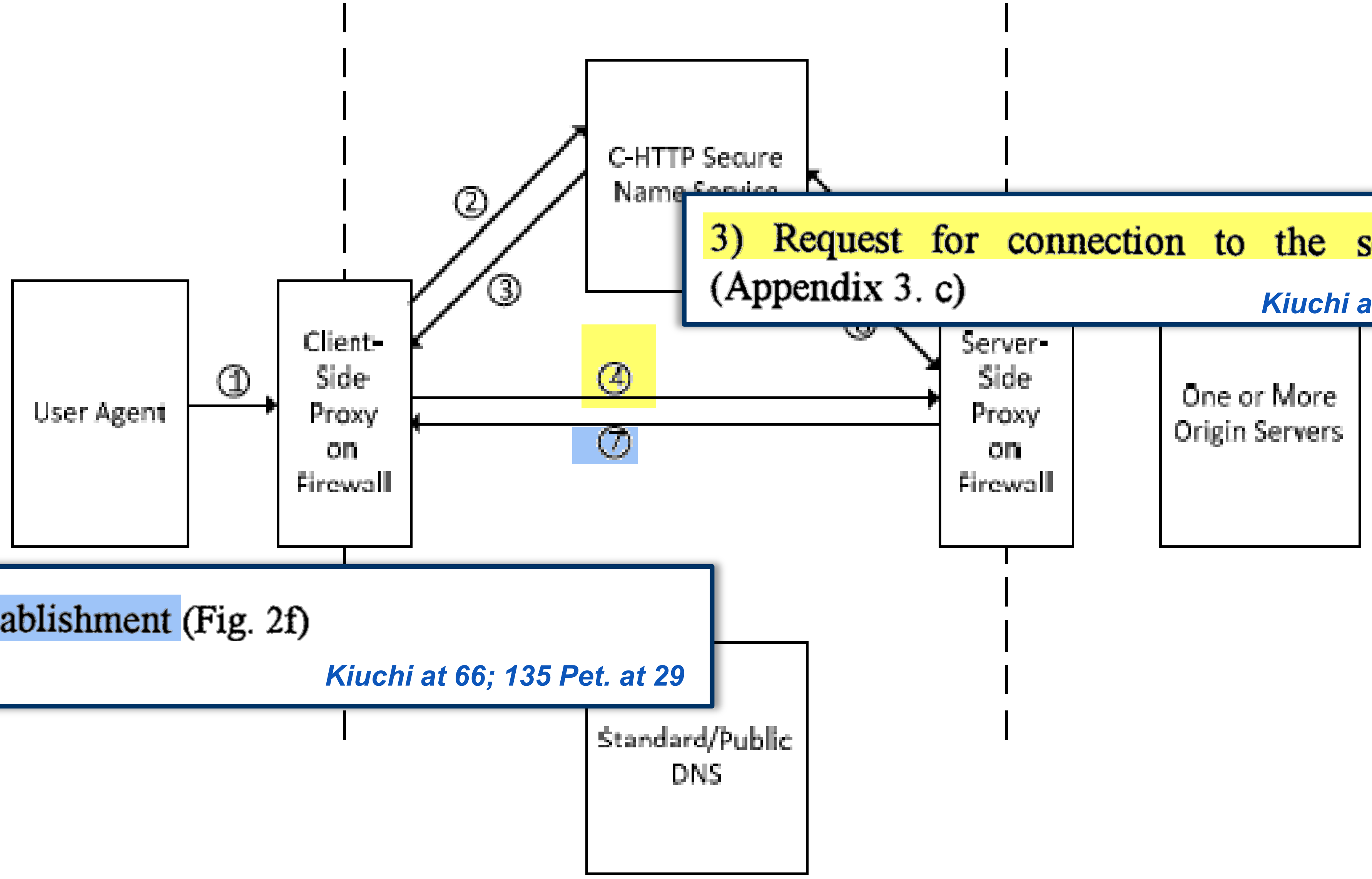
1. My name is Dr. Roch Guerin. I am the chair of the Computer Scienc Engineering department at Washington University in St. Louis. I have been as to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior references relating to its subject matter. My current *curriculum vitae* is attac and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) PhD (1986) in electrical engineering from The California Institute of Technol in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I wa research staff member within the Communication Department, where I worke design and evaluate high-speed switches and networks. From 1990 to 1991, I w research staff member within the IBM High Performance Computing

Mangrove 1

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet


C-HTTP Secure Name Service
User Agent
Client-Side Proxy on Firewall
Server-Side Proxy on Firewall
One or More Origin Servers
Standard/Public DNS
①
②
③
④
⑦

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

Kiuchi at 65; 135 Pet. at 28-29

5) Connection establishment (Fig. 2f)

Kiuchi at 66; 135 Pet. at 29

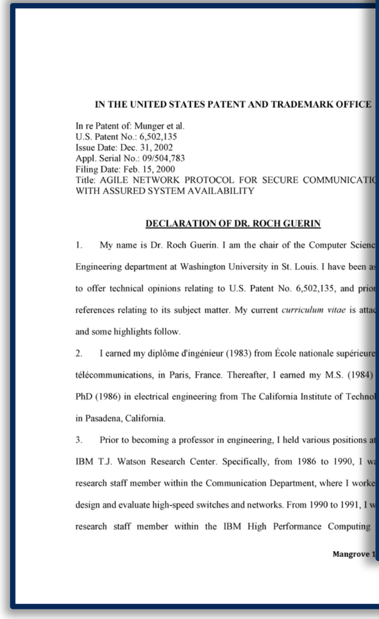
Diagram 2

135 Pet. (Paper 5) at 20

Kiuchi

“*transparently creating*” or “*automatically initiating*” the VPN

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 6,502,135
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIC
WITH ASSURED SYSTEM AVAILABILITY

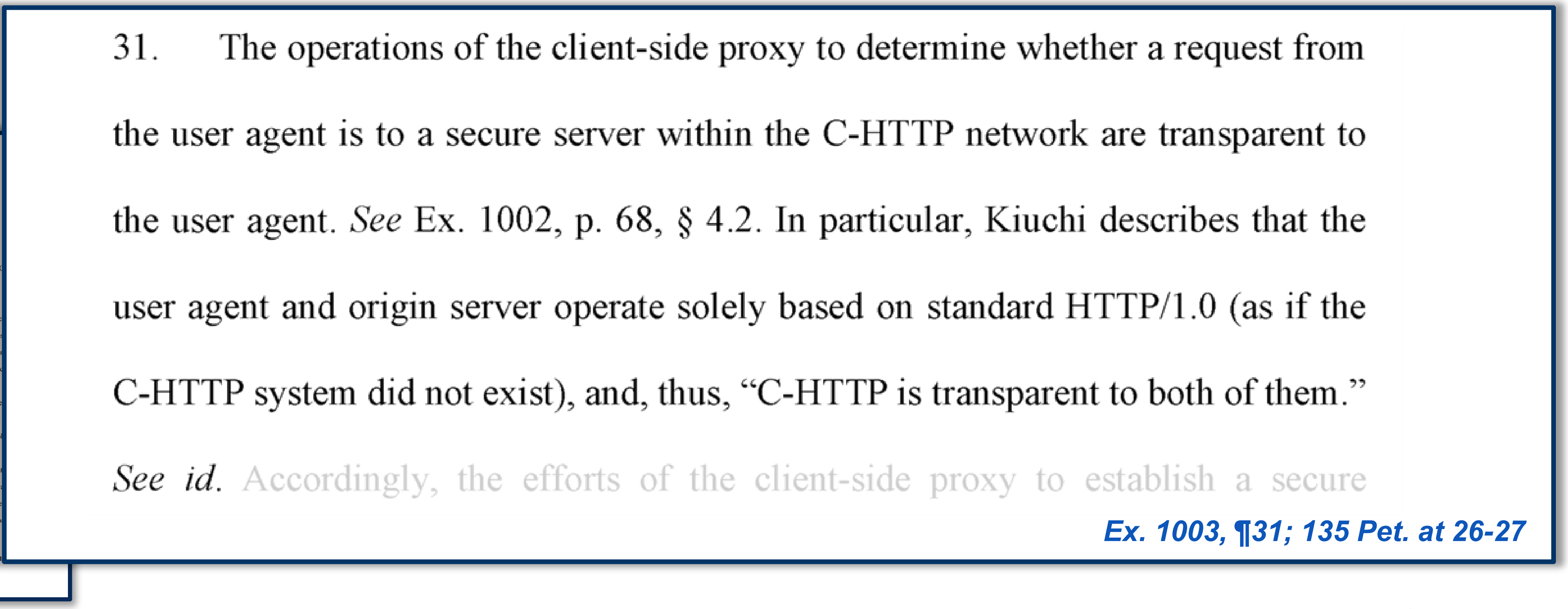
DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Scienc Engineering department at Washington University in St. Louis. I have been as to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior references relating to its subject matter. My current *curriculum vitae* is attac and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) PhD (1986) in electrical engineering from The California Institute of Technol in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I wa research staff member within the Communication Department, where I worke design and evaluate high-speed switches and networks. From 1990 to 1991, I w research staff member within the IBM High Performance Computing

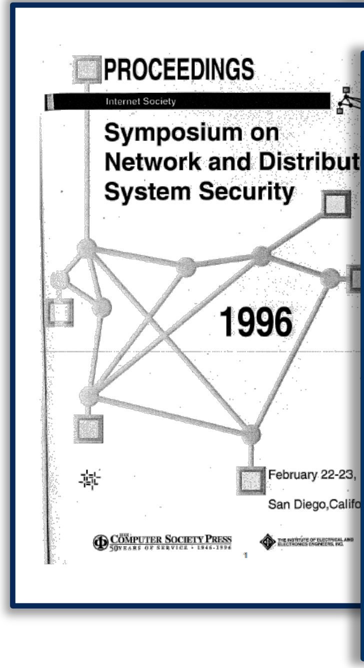
Mangrove 1



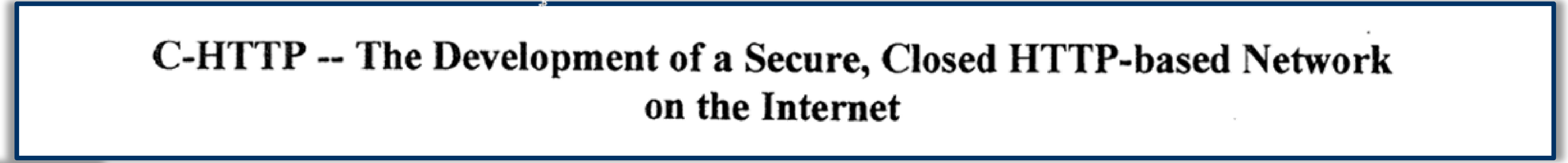
31. The operations of the client-side proxy to determine whether a request from the user agent is to a secure server within the C-HTTP network are transparent to the user agent. *See* Ex. 1002, p. 68, § 4.2. In particular, Kiuchi describes that the user agent and origin server operate solely based on standard HTTP/1.0 (as if the C-HTTP system did not exist), and, thus, “C-HTTP is transparent to both of them.” *See id.* Accordingly, the efforts of the client-side proxy to establish a secure

Ex. 1003, ¶31; 135 Pet. at 26-27

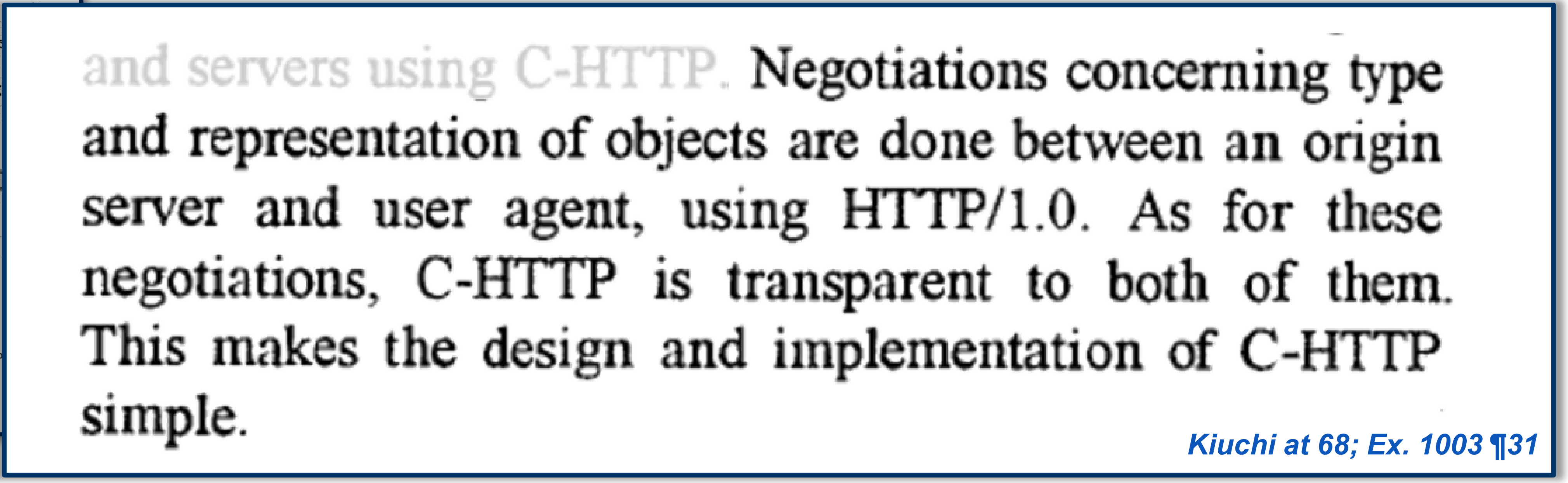
Kiuchi
Ex. 1002



PROCEEDINGS
Internet Society
Symposium on
Network and Distribut
System Security
1996
February 22-23,
San Diego,Califo
COMPUTER SOCIETY PRESS



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

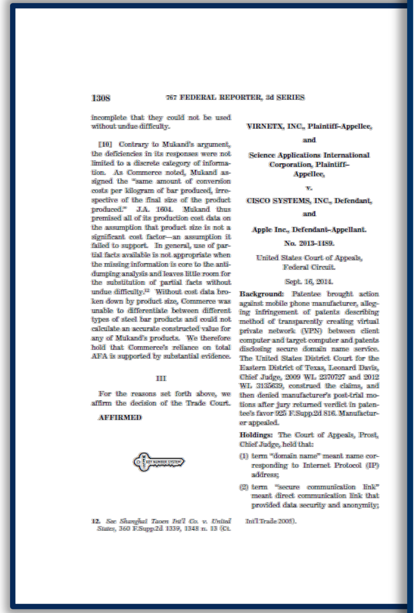


and servers using C-HTTP. Negotiations concerning type and representation of objects are done between an origin server and user agent, using HTTP/1.0. As for these negotiations, C-HTTP is transparent to both of them. This makes the design and implementation of C-HTTP simple.

Kiuchi at 68; Ex. 1003 ¶31

VirnetX v. Cisco, 767 F.3d 1308 (Fed. Cir. 2014)

***VirnetX v. Cisco* (Fed. Cir. 2014)**



1308 767 FEDERAL REPORTER, 3d SERIES

incomplete that they could not be used without undue difficulty.

[10] Contrary to Mukand's argument, the deficiencies in its responses were not limited to a discrete category of information. As Commerce noted, Mukand assigned the "same amount of conversion costs per kilogram of bar produced, irrespective of the final size of the product produced." J.A. 1604. Mukand thus premised all of its production cost data on the assumption that product size is not a significant cost factor—an assumption it failed to support. In general, use of partial facts available is not appropriate when the missing information is core to the antidumping analysis and leaves little room for the substitution of partial facts without undue difficulty.[12] Without cost data broken down by product size, Commerce was unable to differentiate between different types of steel bar products and could not calculate an accurate constructed value for any of Mukand's products. We therefore hold that Commerce's reliance on total AFA is supported by substantial evidence.

III

For the reasons set forth above, we affirm the decision of the Trade Court.

AFFIRMED

VIRNETX, INC., Plaintiff–Appellee,

and

Science Applications International Corporation, Plaintiff–Appellee,

v.

CISCO SYSTEMS, INC., Defendant,

and

Apple Inc., Defendant–Appellant.

No. 2013–1489.

United States Court of Appeals, Federal Circuit.

Sept. 16, 2014.

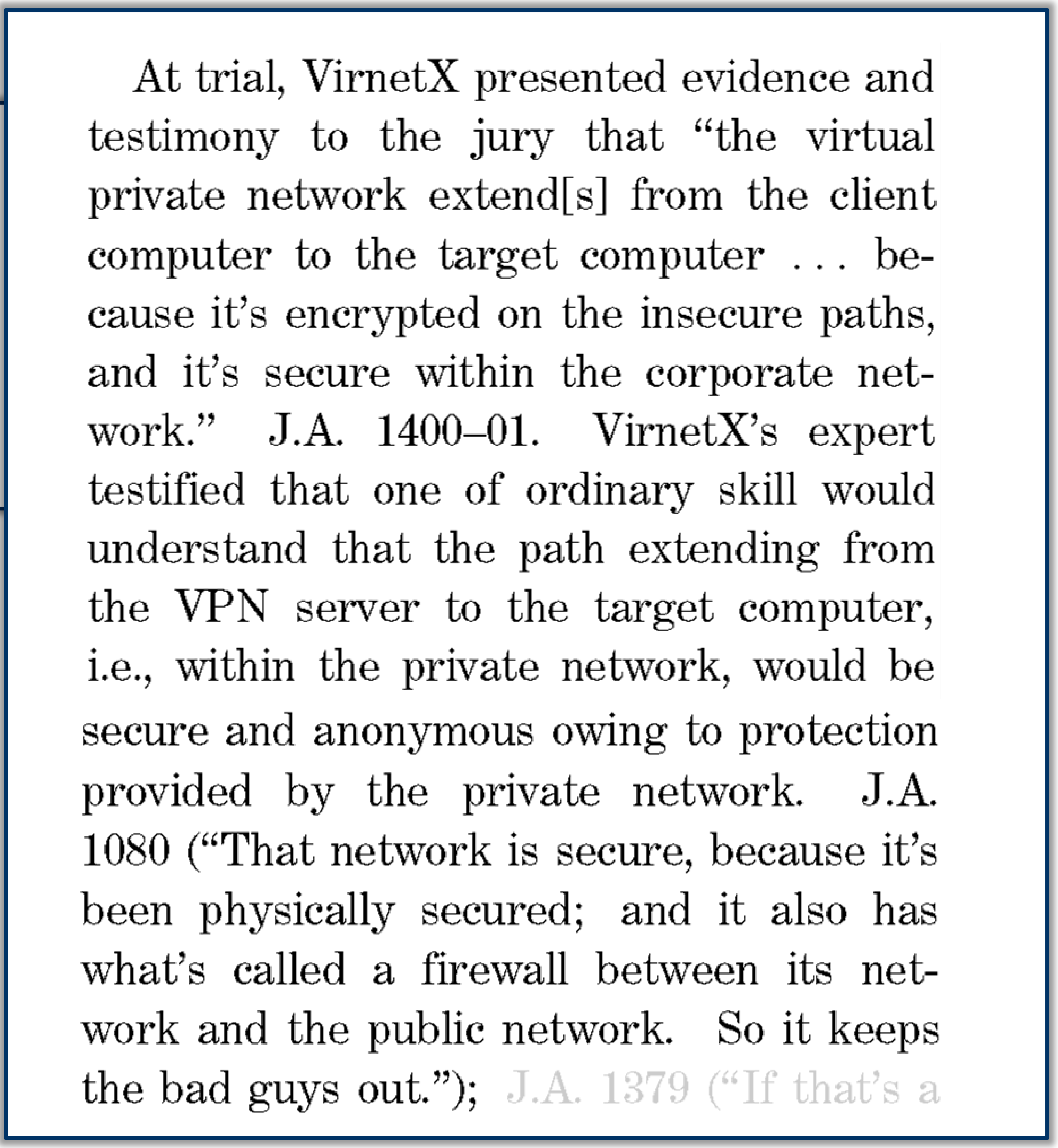
Background: Patentee brought action against mobile phone manufacturer, alleging infringement of patents describing method of transparently creating virtual private network (VPN) between client computer and target computer and patents disclosing secure domain name service. The United States District Court for the Eastern District of Texas, Leonard Davis, Chief Judge, 2009 WL 2370727 and 2012 WL 3135639, construed the claims, and then denied manufacturer's post-trial motions after jury returned verdict in patentee's favor 925 F.Supp.2d 816. Manufacturer appealed.

Holdings: The Court of Appeals, Prost, Chief Judge, held that:

(1) term "domain name" meant name corresponding to Internet Protocol (IP) address;

(2) term "secure communication link" meant direct communication link that provided data security and anonymity;

[12] *See Shanghai Taoen Int'l Co. v. United States*, 360 F.Supp.2d 1339, 1348 n. 13 (Ct. Int'l Trade 2005).

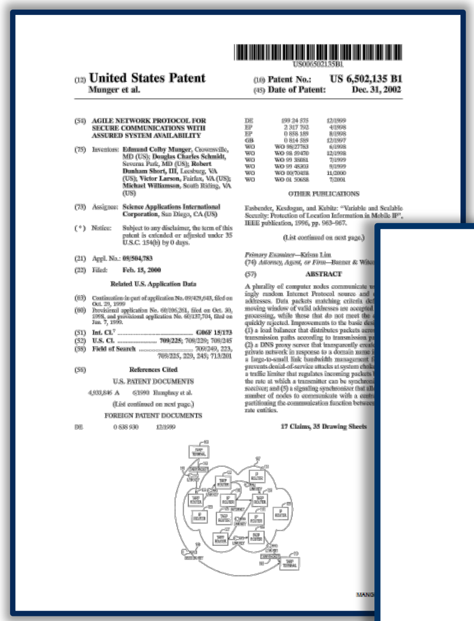


At trial, VirnetX presented evidence and testimony to the jury that "the virtual private network extend[s] from the client computer to the target computer . . . because it's encrypted on the insecure paths, and it's secure within the corporate network." J.A. 1400–01. VirnetX's expert testified that one of ordinary skill would understand that the path extending from the VPN server to the target computer, i.e., within the private network, would be secure and anonymous owing to protection provided by the private network. J.A. 1080 ("That network is secure, because it's been physically secured; and it also has what's called a firewall between its network and the public network. So it keeps the bad guys out."); J.A. 1379 ("If that's a

VirnetX, 767 F.3d at 1321
135 Reply at 12
151 Reply at 14

135 Patent: Claim 7

135 Patent
Ex. 1001



US006502135B1

(12) **United States Patent**
Munger et al.

(10) **Patent No.:** **US 6,502,135 B1**
(45) **Date of Patent:** **Dec. 31, 2002**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY**

(75) Inventors: **Edmund Colby Munger**, Crownsville, MD (US); **Douglas Charles Schmidt**, Severna Park, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Science Applications International Corporation**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/504,783**

(22) Filed: **Feb. 15, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**⁷ **G06F 15/173**

(52) **U.S. Cl.** **709/225**; 709/229; 709/245

(58) **Field of Search** 709/249, 223, 709/225, 229, 245; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication, 1996, pp. 963–967.

(List continued on next page.)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witc

(57) **ABSTRACT**

A plurality of computer nodes communicate u ingly random Internet Protocol source and addresses. Data packets matching criteria def moving window of valid addresses are accepted processing, while those that do not meet the quickly rejected. Improvements to the basic desi (1) a load balancer that distributes packets acro transmission paths according to transmission pa (2) a DNS proxy server that transparently creat private network in response to a domain name i a large-to-small link bandwidth management f prevents denial-of-service attacks at system chok a traffic limiter that regulates incoming packets the rate at which a transmitter can be synchroni receiver; and (5) a signaling synchronizer that all number of nodes to communicate with a centr partitioning the communication function betwee rate entities.

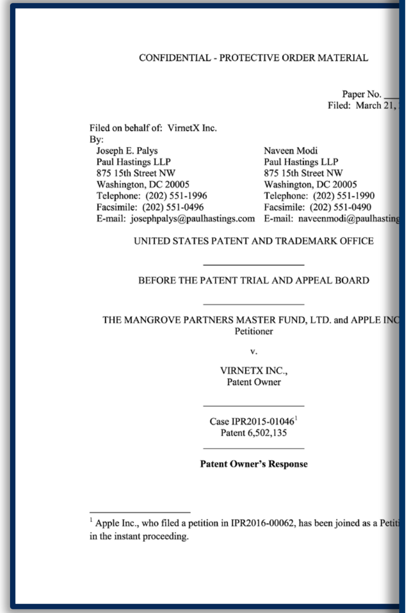
17 Claims, 35 Drawing Sheets

MANG

7. The method of claim **1**, wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer.

Gatekeeper and DNS Server Can Be on Same Device

Patent Owner's Response



CONFIDENTIAL - PROTECTIVE ORDER MATERIAL

Paper No. ___
Filed: March 21,

Filed on behalf of: VirnetX Inc.
By:

Joseph E. Palys	Naveen Modi
Paul Hastings LLP	Paul Hastings LLP
875 15th Street NW	875 15th Street NW
Washington, DC 20005	Washington, DC 20005
Telephone: (202) 551-1996	Telephone: (202) 551-1990
Facsimile: (202) 551-0496	Facsimile: (202) 551-0490
E-mail: josephpalys@paulhastings.com	E-mail: naveenmodi@paulhasting

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD. and APPLE INC
Petitioner

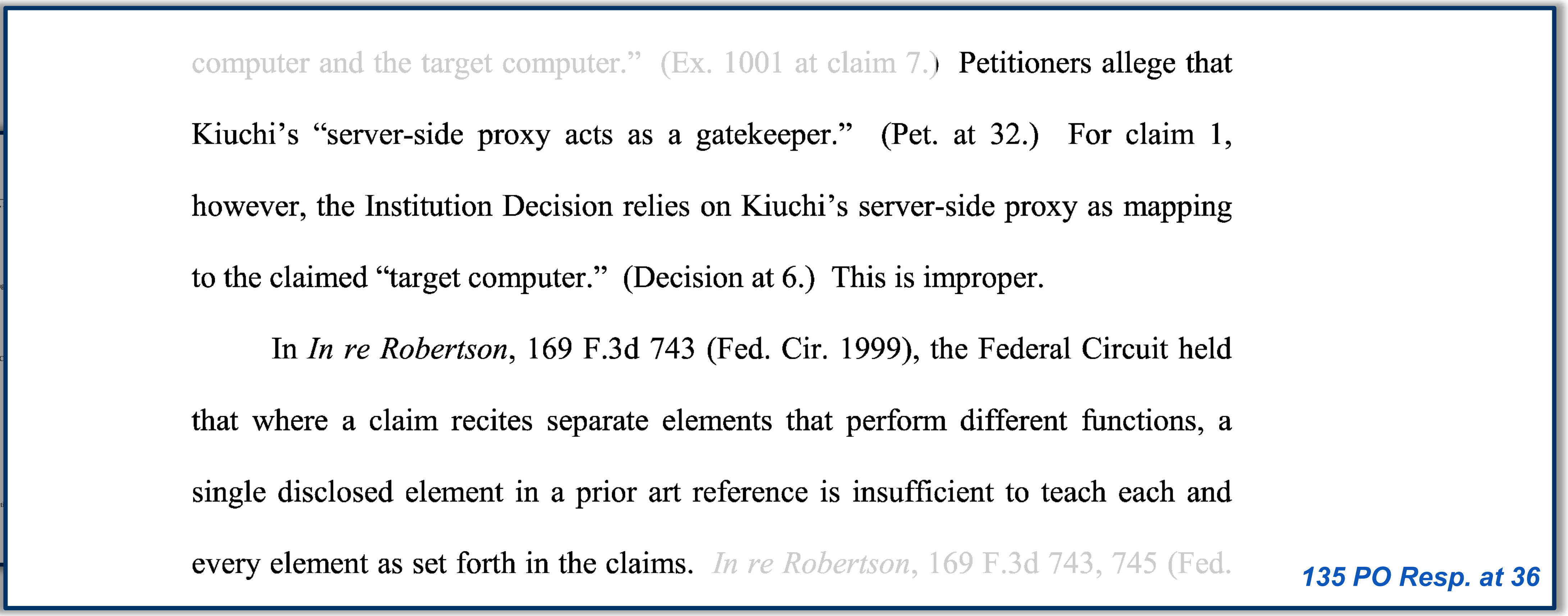
v.

VIRNETX INC.,
Patent Owner

Case IPR2015-01046[1]
Patent 6,502,135

Patent Owner's Response

[1] Apple Inc., who filed a petition in IPR2016-00062, has been joined as a Petiti in the instant proceeding.

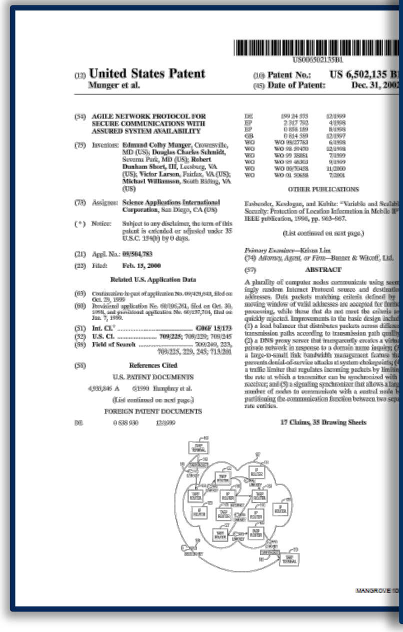


computer and the target computer." (Ex. 1001 at claim 7.) Petitioners allege that Kiuchi's "server-side proxy acts as a gatekeeper." (Pet. at 32.) For claim 1, however, the Institution Decision relies on Kiuchi's server-side proxy as mapping to the claimed "target computer." (Decision at 6.) This is improper.

In *In re Robertson*, 169 F.3d 743 (Fed. Cir. 1999), the Federal Circuit held that where a claim recites separate elements that perform different functions, a single disclosed element in a prior art reference is insufficient to teach each and every element as set forth in the claims. *In re Robertson*, 169 F.3d 743, 745 (Fed.

135 PO Resp. at 36

135 Patent Ex. 1001



(12) **United States Patent**
Munger et al.

(10) **Patent No.: US 6,502,135 B1**
(45) **Date of Patent: Dec. 31, 2002**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY**

(75) Inventors: **Edmund Colby Munger**, Crownsville, MD (US); **Douglas Charles Schmidt**, Severna Park, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Science Applications International Corporation**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/504,783**

(22) Filed: **Feb. 15, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**7 .... **G06F 15/173**
(52) **U.S. Cl.** **709/225**; 709/229; 709/245
(58) **Field of Search** 709/249, 223, 709/225, 229, 245; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE	0 838 930	12/1999
DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

OTHER PUBLICATIONS

Fasbender, Kesdogan, and Kubitz: "Variable and Scalabl Security: Protection of Location Information in Mobile IP" IEEE publication, 1996, pp. 963–967.

(List continued on next page.)

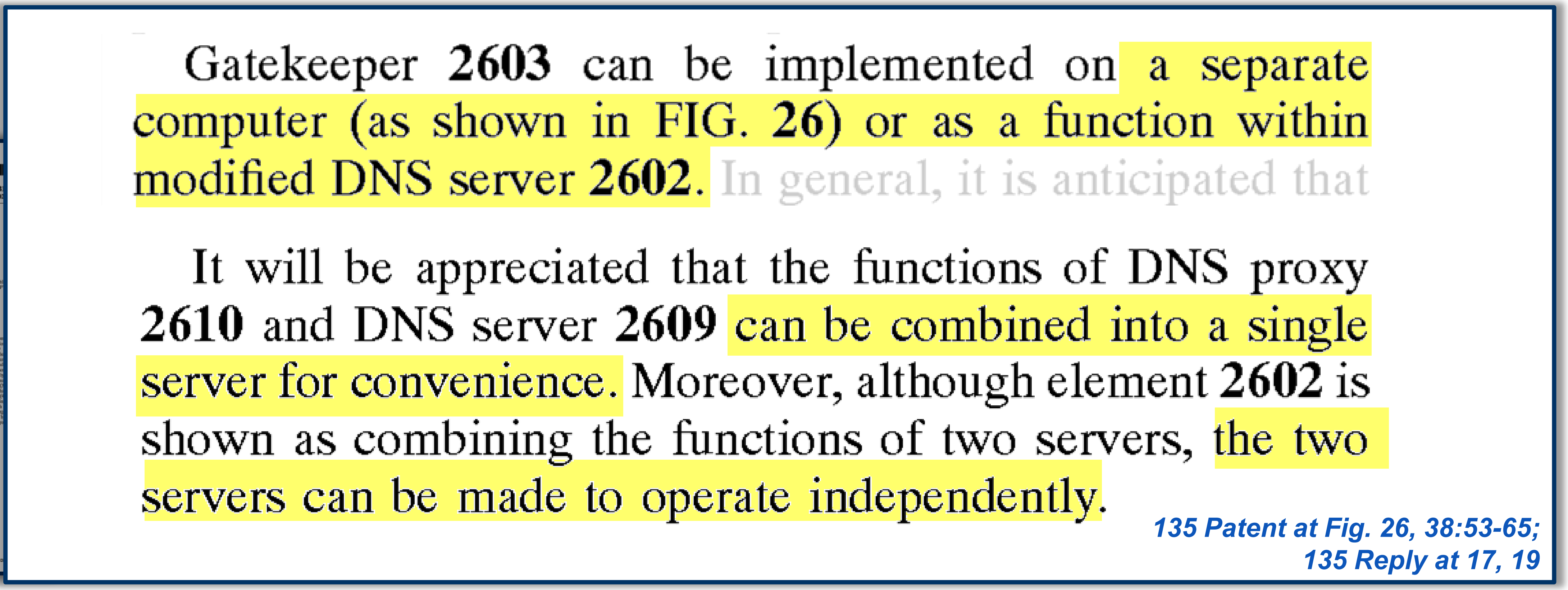
Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(57) **ABSTRACT**

A plurality of computer nodes communicate using seem ingly random Internet Protocol source and destinatio addresses. Data packets matching criteria defined by moving window of valid addresses are accepted for furthe processing, while those that do not meet the criteria ar quickly rejected. Improvements to the basic design includ (1) a load balancer that distributes packets across differen transmission paths according to transmission path quality (2) a DNS proxy server that transparently creates a virtua private network in response to a domain name inquiry; (a large-to-small link bandwidth management feature th prevents denial-of-service attacks at system chokepoints; (a traffic limiter that regulates incoming packets by limitin the rate at which a transmitter can be synchronized with receiver; and (5) a signaling synchronizer that allows a larg number of nodes to communicate with a central node b partitioning the communication function between two sepa rate entities.

17 Claims, 35 Drawing Sheets

MANGROVE 10



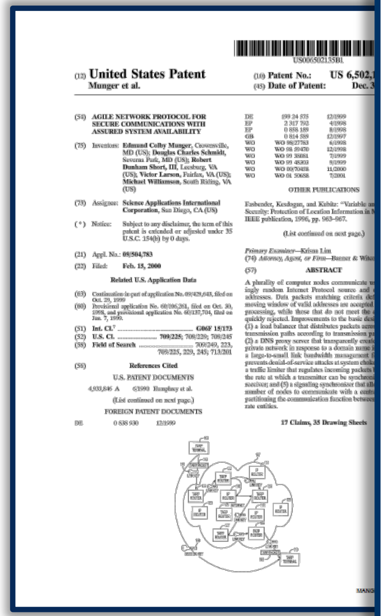
Gatekeeper **2603** can be implemented on a separate computer (as shown in FIG. **26**) or as a function within modified DNS server **2602**. In general, it is anticipated that

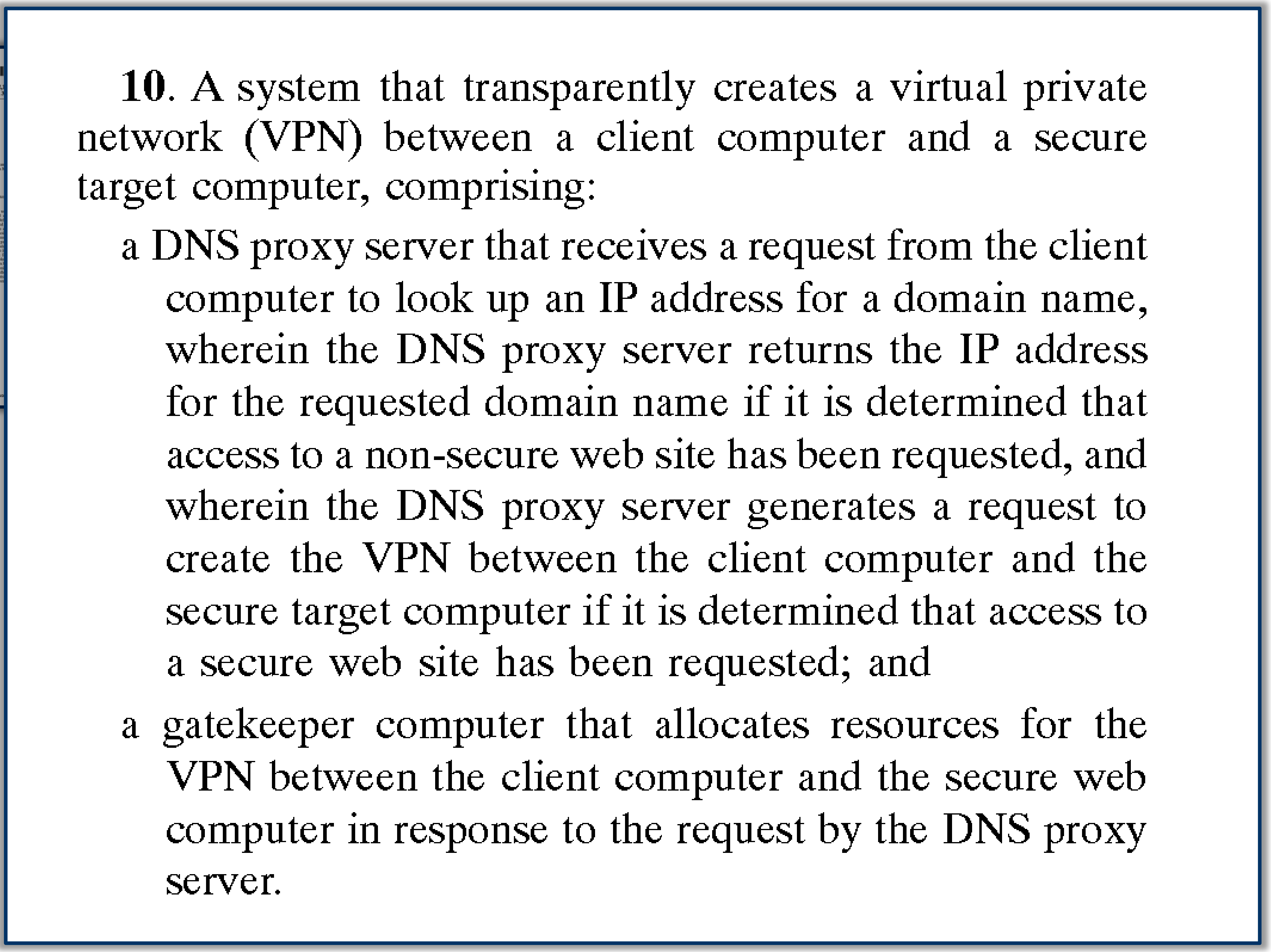
It will be appreciated that the functions of DNS proxy **2610** and DNS server **2609** can be combined into a single server for convenience. Moreover, although element **2602** is shown as combining the functions of two servers, the two servers can be made to operate independently.

135 Patent at Fig. 26, 38:53-65; 135 Reply at 17, 19

135 Patent: Claim 10

135 Patent
Ex. 1001





10. A system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer, comprising:

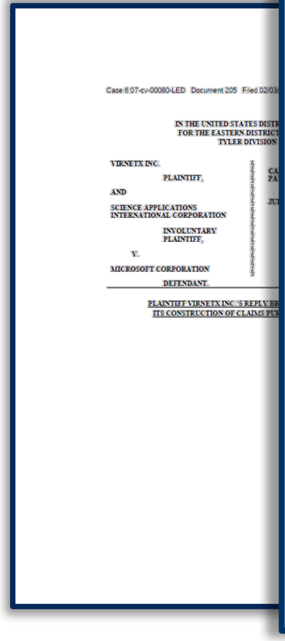
a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested; and

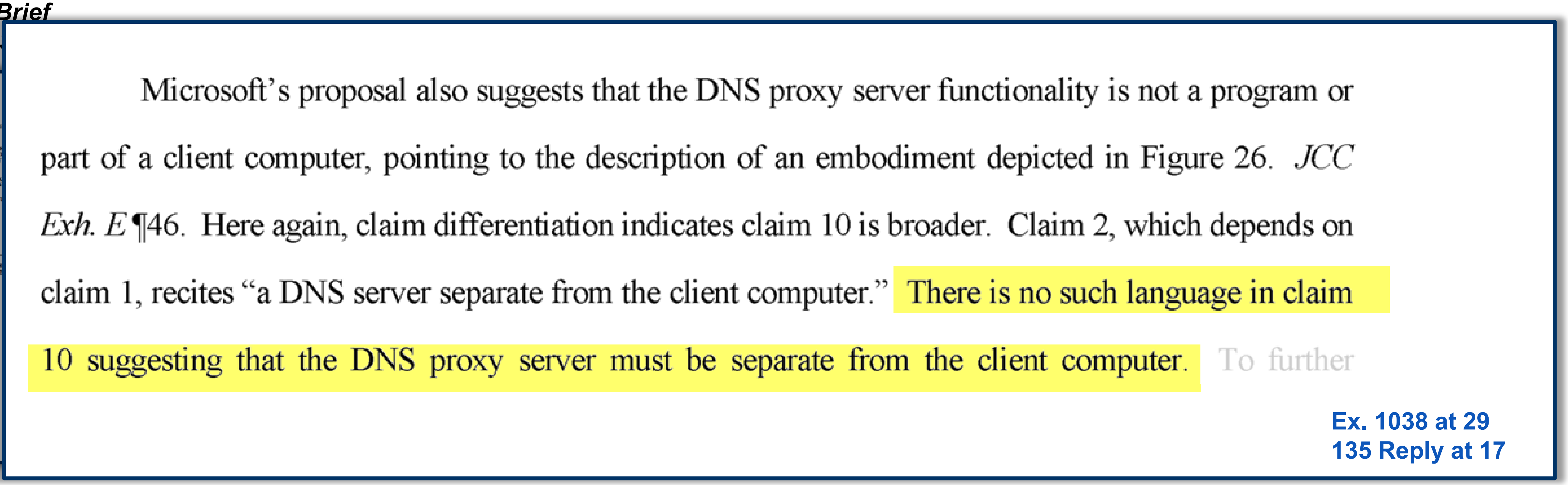
a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server.

DNS Proxy Server and Client Can Be on Same Device

Ex. 1038 – Plaintiff VirnetX's Opening Brief ISO Construction of Claims

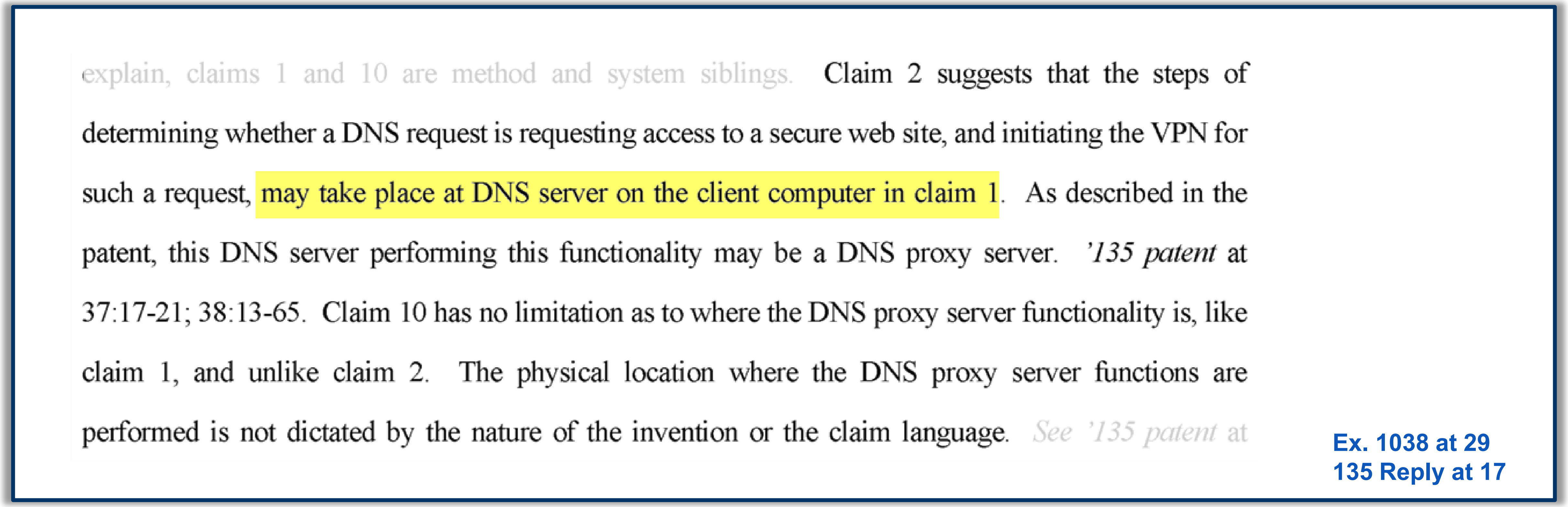
VirnetX Brief
Ex. 10





Microsoft's proposal also suggests that the DNS proxy server functionality is not a program or part of a client computer, pointing to the description of an embodiment depicted in Figure 26. *JCC Exh. E* ¶46. Here again, claim differentiation indicates claim 10 is broader. Claim 2, which depends on claim 1, recites "a DNS server separate from the client computer." There is no such language in claim 10 suggesting that the DNS proxy server must be separate from the client computer. To further

Ex. 1038 at 29
135 Reply at 17

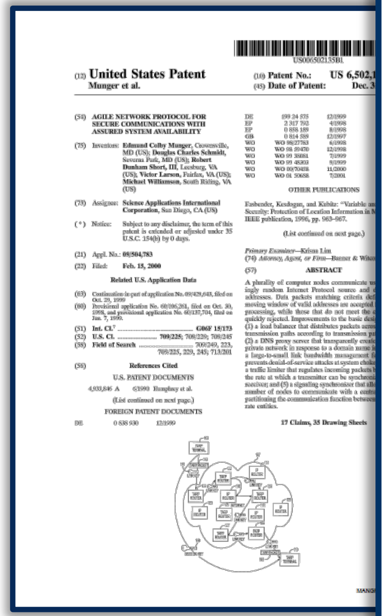


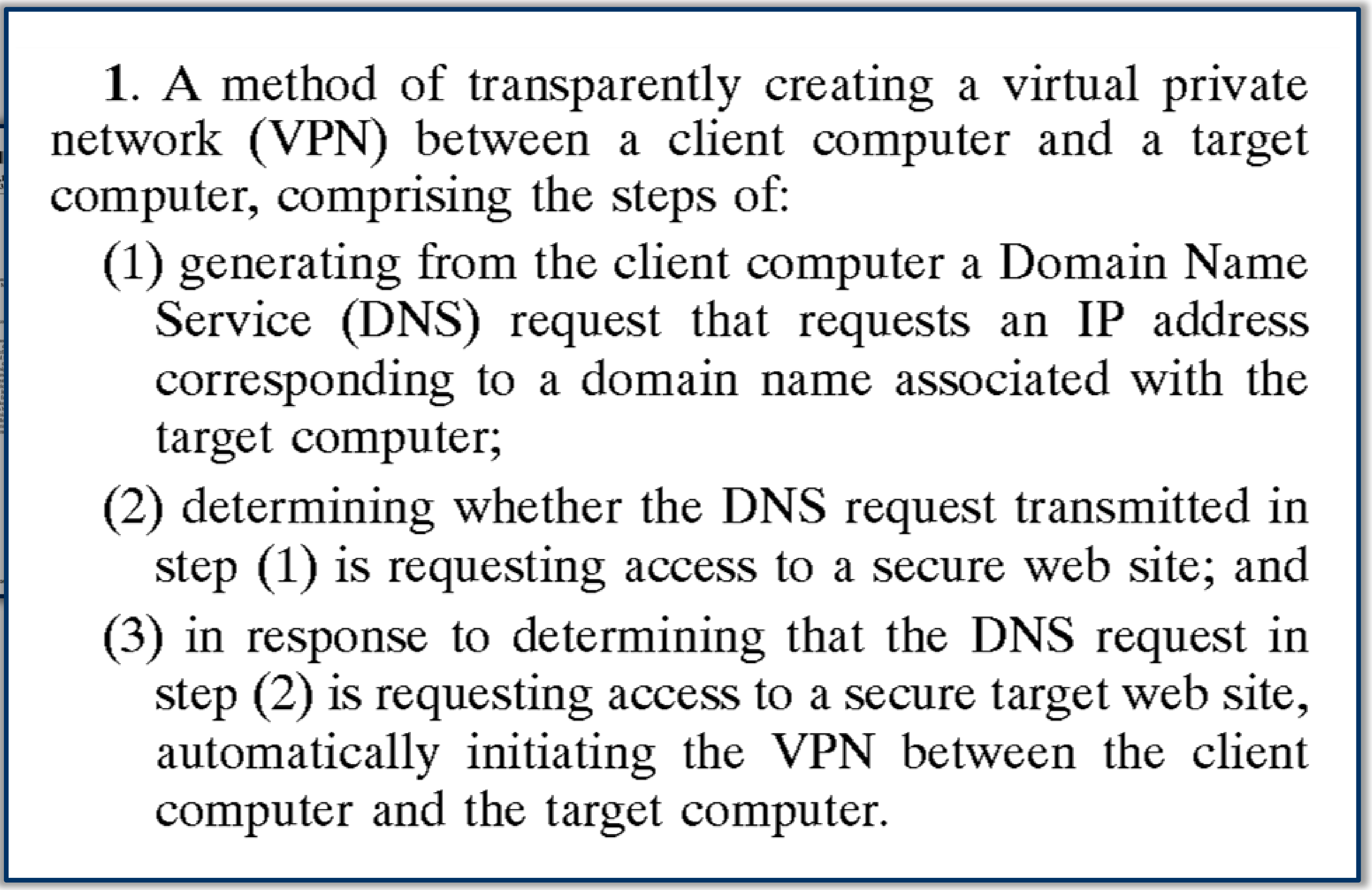
explain, claims 1 and 10 are method and system siblings. Claim 2 suggests that the steps of determining whether a DNS request is requesting access to a secure web site, and initiating the VPN for such a request, may take place at DNS server on the client computer in claim 1. As described in the patent, this DNS server performing this functionality may be a DNS proxy server. *'135 patent* at 37:17-21; 38:13-65. Claim 10 has no limitation as to where the DNS proxy server functionality is, like claim 1, and unlike claim 2. The physical location where the DNS proxy server functions are performed is not dictated by the nature of the invention or the claim language. *See '135 patent* at

Ex. 1038 at 29
135 Reply at 17

135 Patent: Claims 1 & 2

135 Patent
Ex. 1001



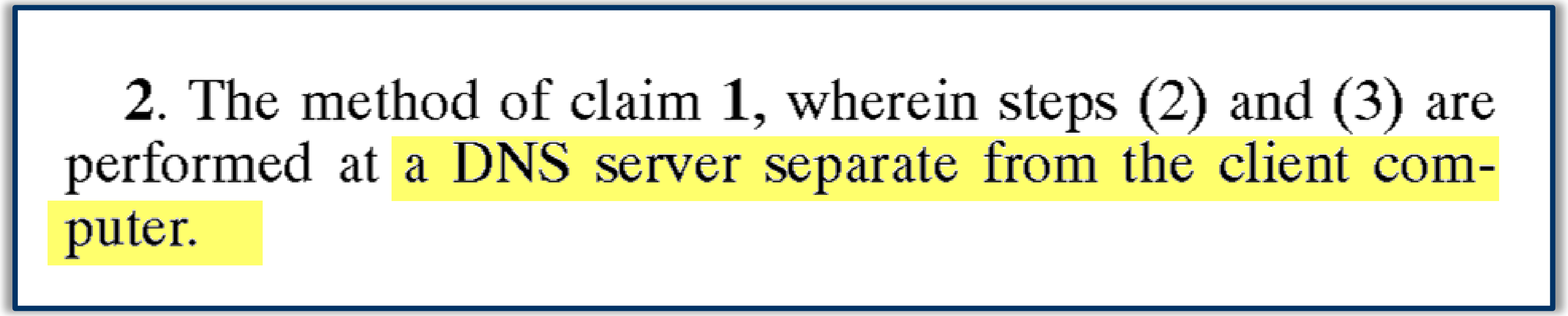


1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

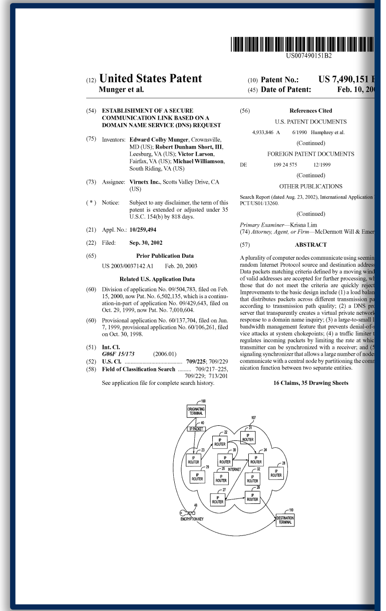
(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.



2. The method of claim **1**, wherein steps (2) and (3) are performed at a DNS server separate from the client computer.

151 Patent

151 Patent
Ex. 1001



US007490151B2

(12) **United States Patent**
Munger et al.

(10) **Patent No.:** **US 7,490,151 I**
(45) **Date of Patent:** **Feb. 10, 20**

(54) **ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST**

(75) Inventors: **Edward Colby Munger**, Crownsville, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/259,494**

(22) Filed: **Sep. 30, 2002**

(65) **Prior Publication Data**

US 2003/0037142 A1 Feb. 20, 2003

Related U.S. Application Data

(60) Division 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.** **709/225**; 709/229
(58) **Field of Classification Search** 709/217–225, 709/229; 713/201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Aug. 23, 2002), International Application PCT/US01/13260.

(Continued)

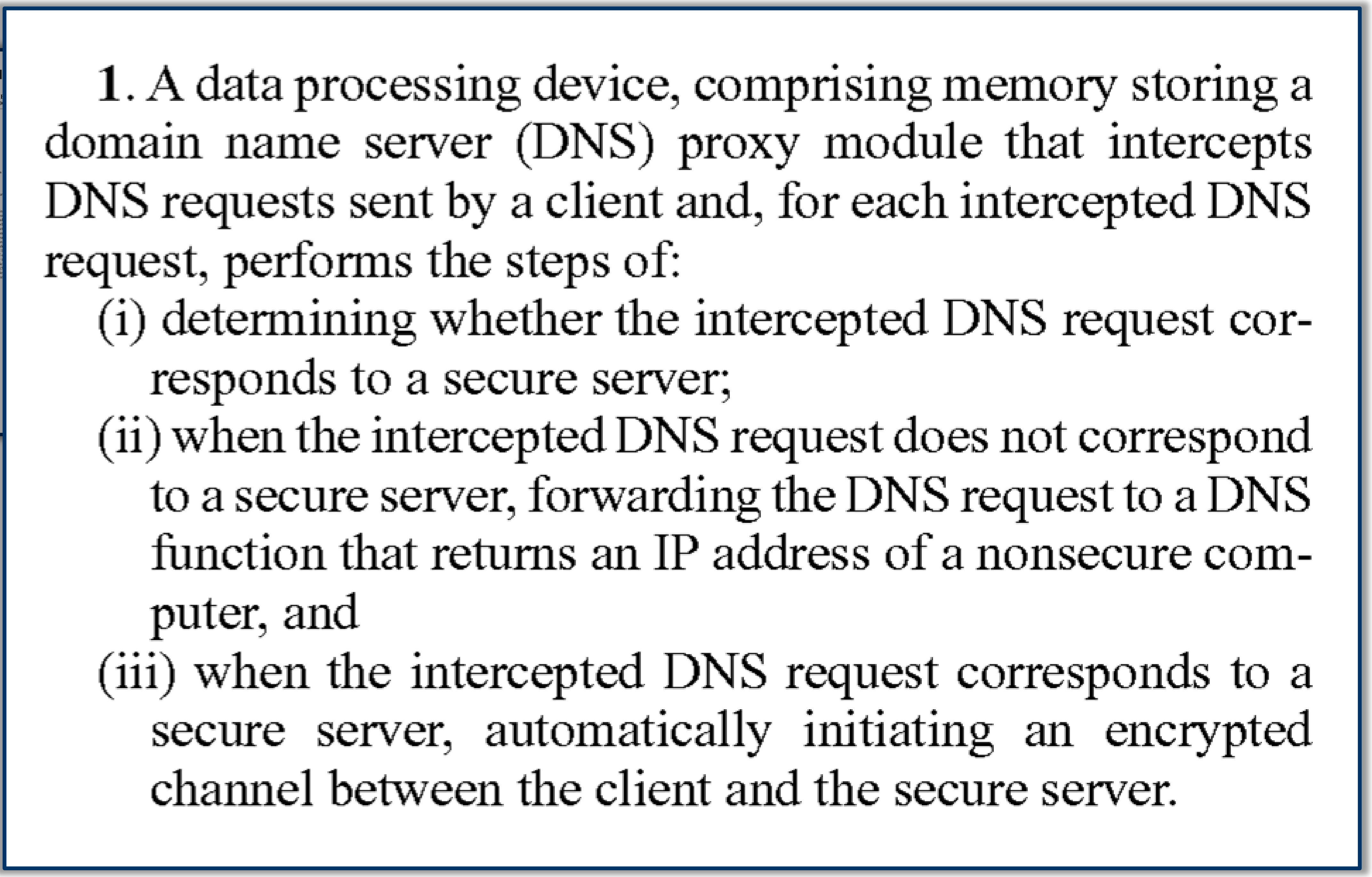
Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emer

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemin random Internet Protocol source and destination address Data packets matching criteria defined by a moving wind of valid addresses are accepted for further processing, wh those that do not meet the criteria are quickly reject Improvements to the basic design include (1) a load balan that distributes packets across different transmission pa according to transmission path quality; (2) a DNS pr server that transparently creates a virtual private network response to a domain name inquiry; (3) a large-to-small l bandwidth management feature that prevents denial-of-s vice attacks at system chokepoints; (4) a traffic limiter t regulates incoming packets by limiting the rate at whic transmitter can be synchronized with a receiver; and (5 signaling synchronizer that allows a large number of node communicate with a central node by partitioning the comm nication function between two separate entities.

16 Claims, 35 Drawing Sheets

100
ORIGINATING TERMINAL
40
IP PACKET
107
31
IP ROUTER
22
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
29
IP ROUTER
25
IP ROUTER
INTERNET
32
IP ROUTER
28
IP ROUTER
27
IP ROUTER
26
IP ROUTER
48
ENCRYPTION KEY
110
DESTINATION TERMINAL



1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

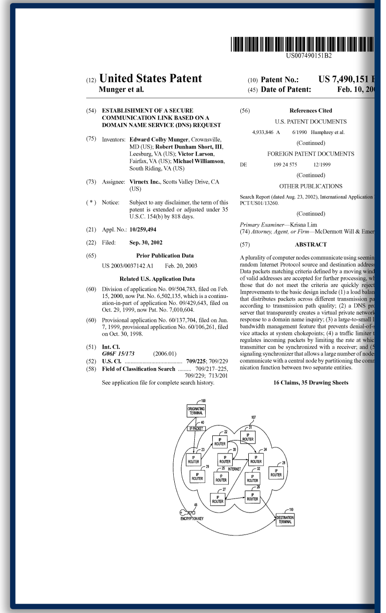
(i) determining whether the intercepted DNS request corresponds to a secure server;

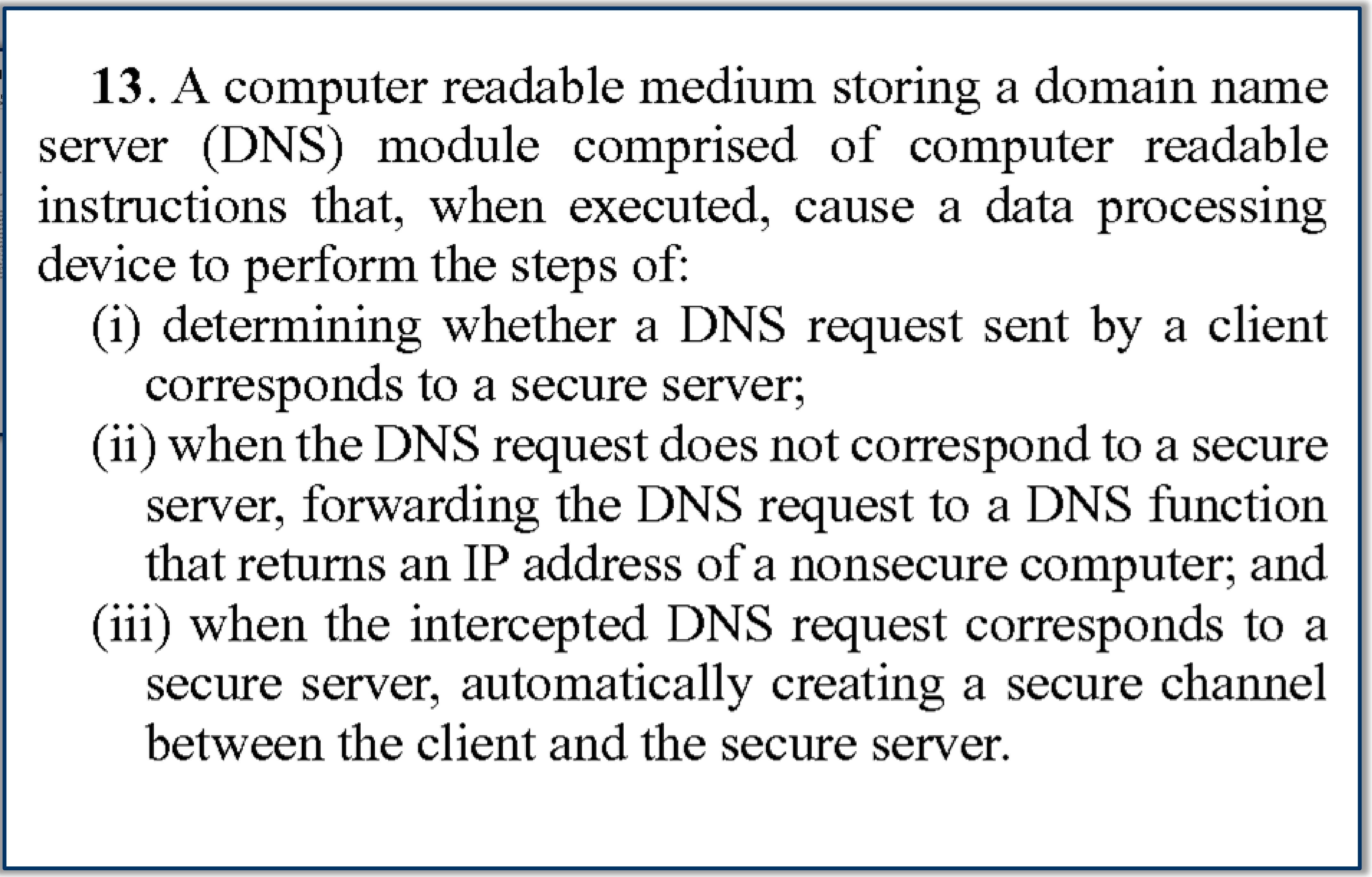
(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.

151 Patent

151 Patent
Ex. 1001





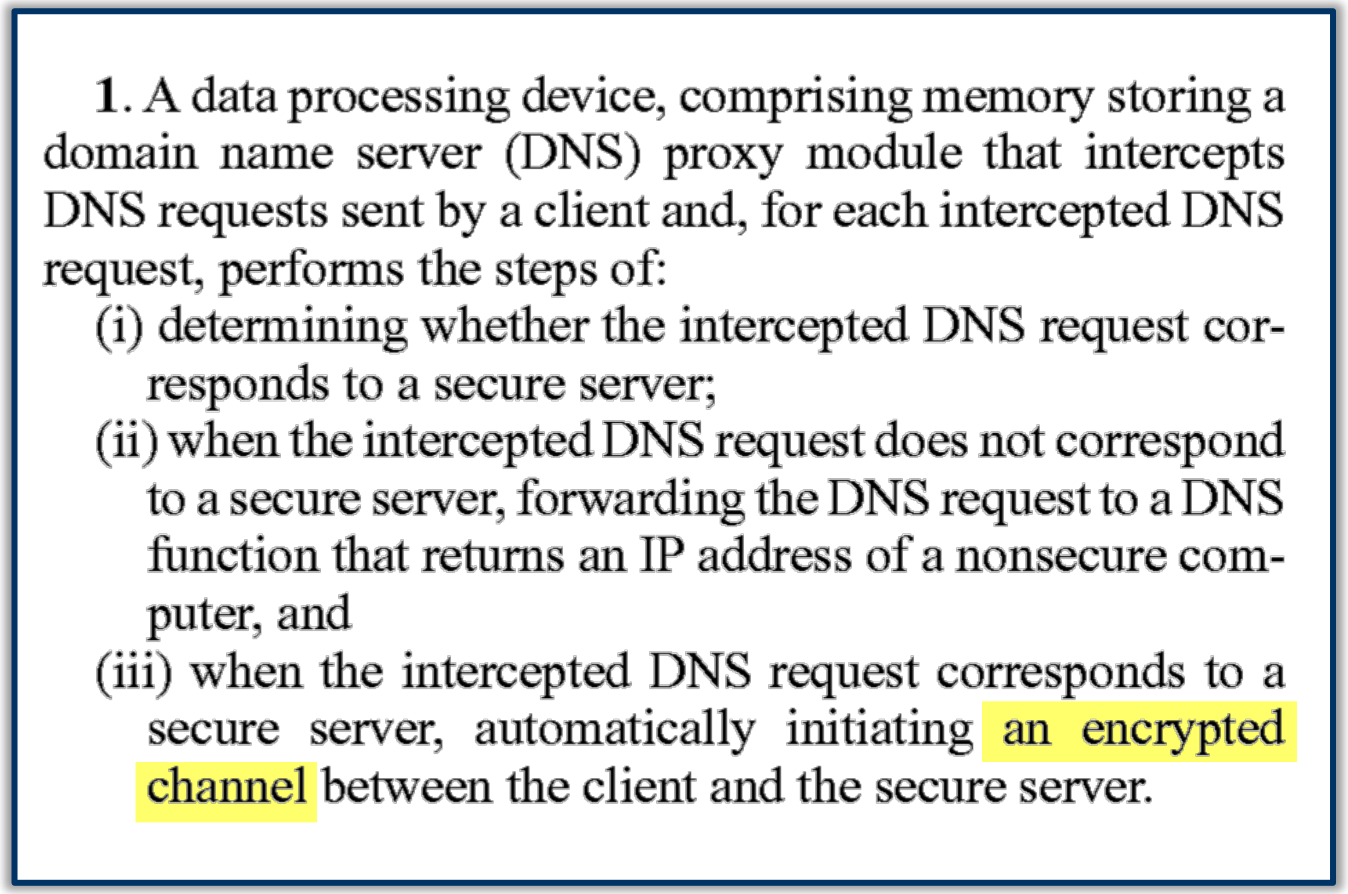
13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

151 Patent

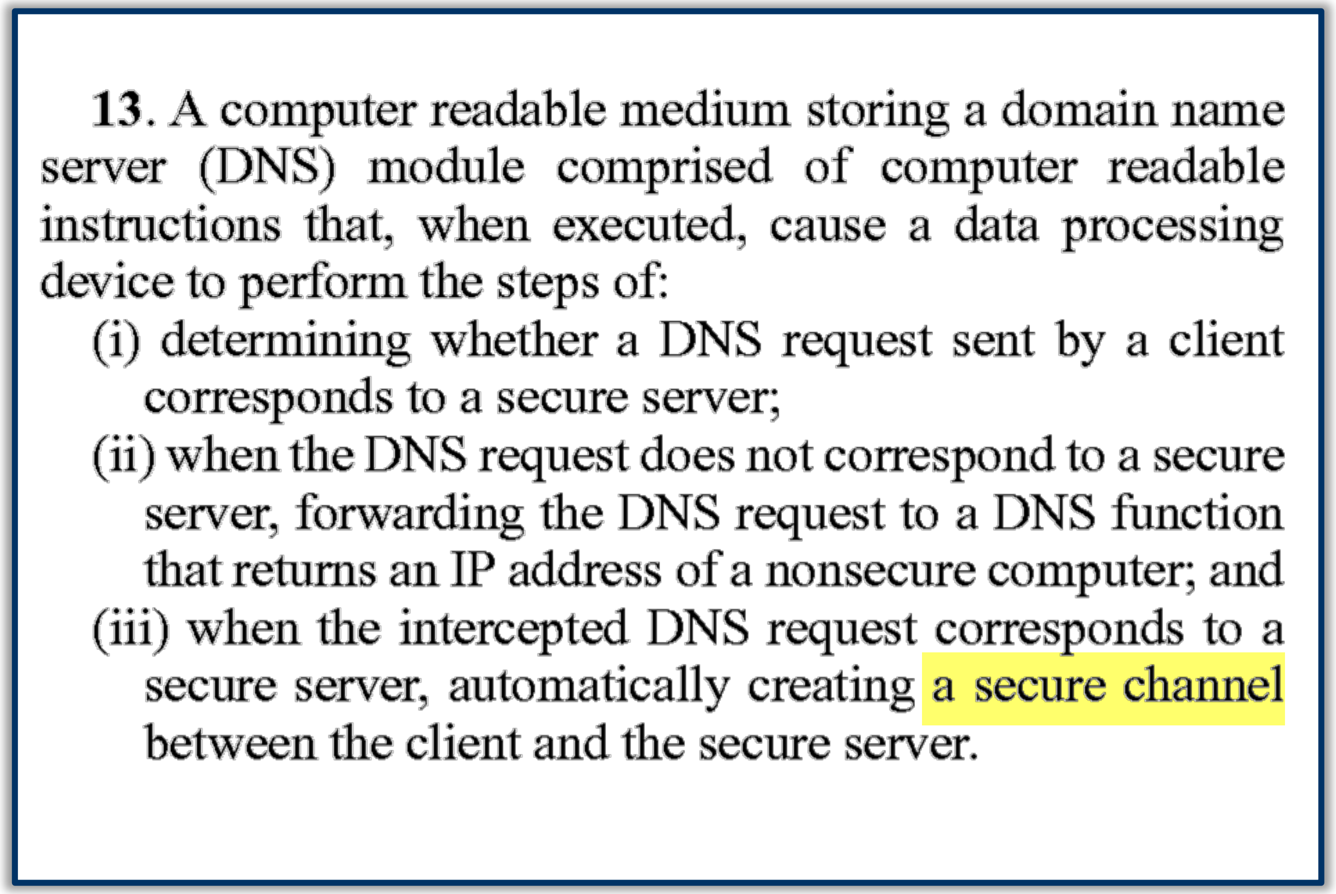


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.

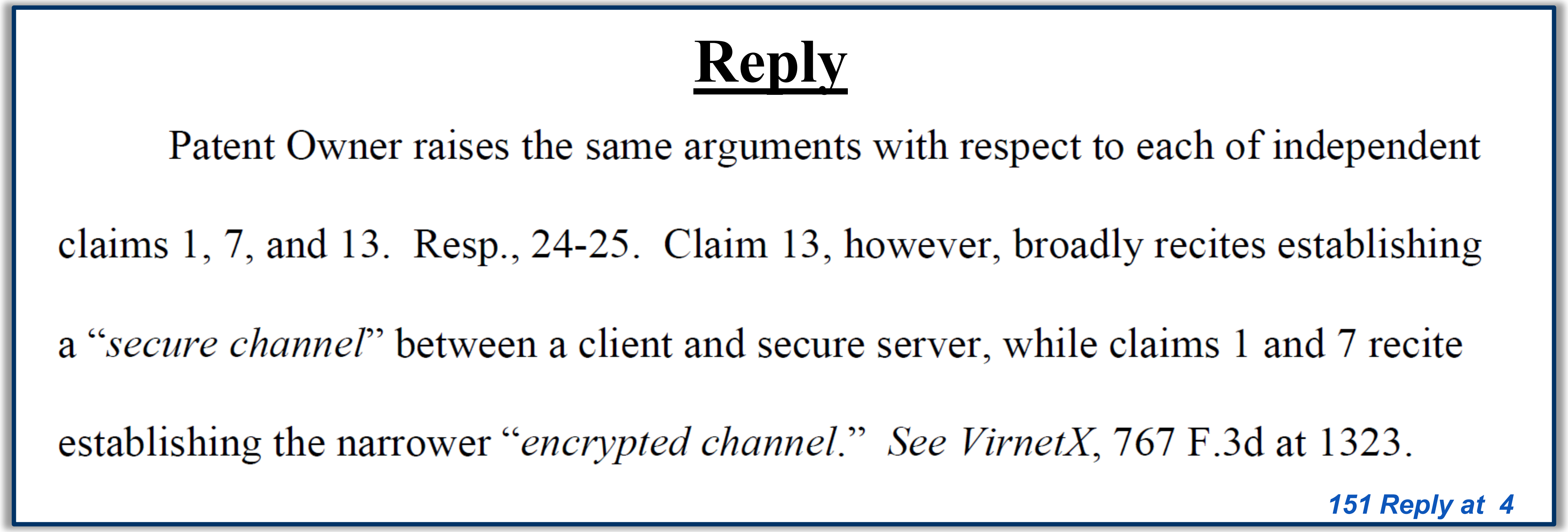


13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

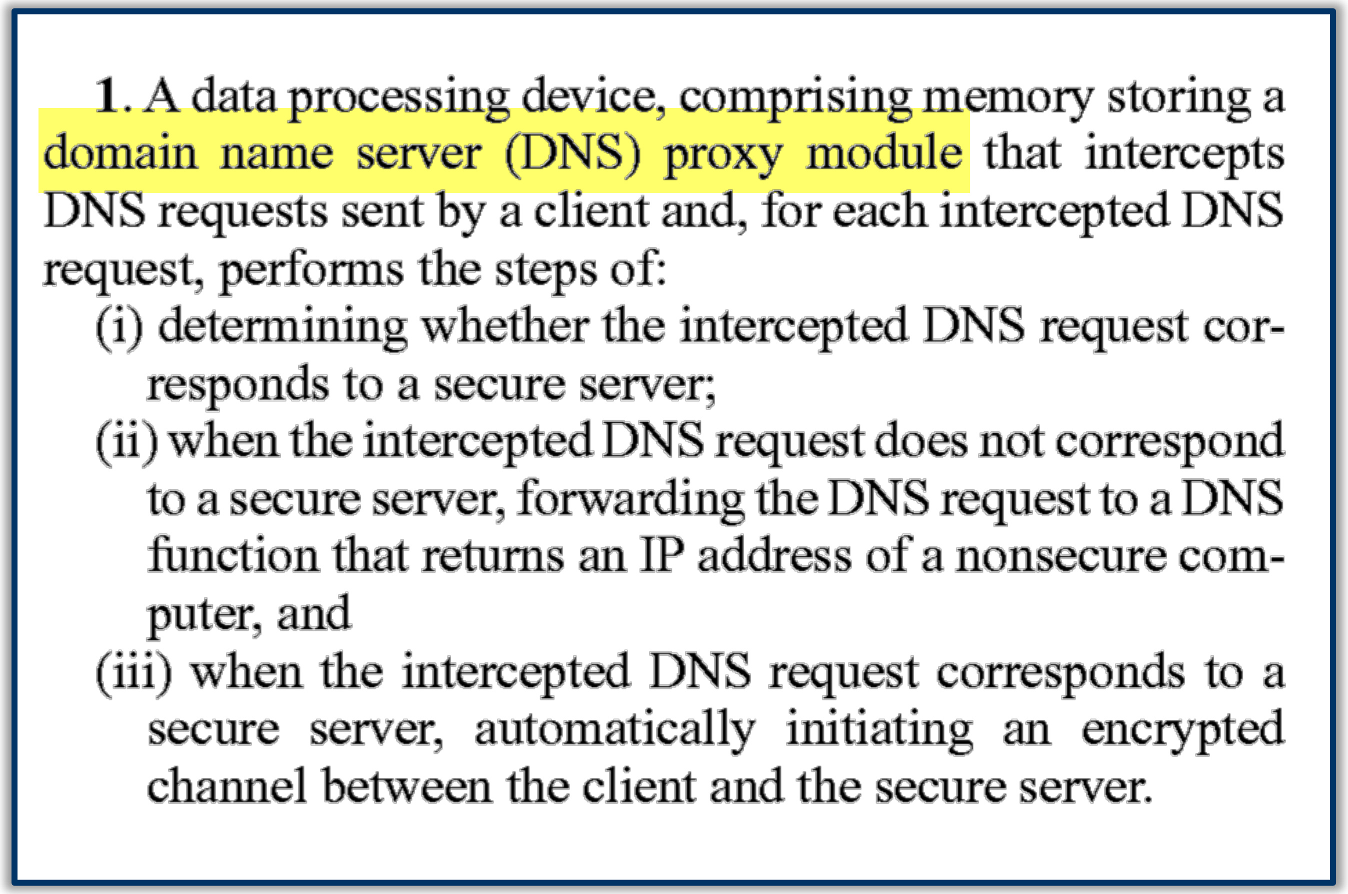


Reply

Patent Owner raises the same arguments with respect to each of independent claims 1, 7, and 13. Resp., 24-25. Claim 13, however, broadly recites establishing a "*secure channel*" between a client and secure server, while claims 1 and 7 recite establishing the narrower "*encrypted channel*." *See VirnetX*, 767 F.3d at 1323.

151 Reply at 4

151 Patent

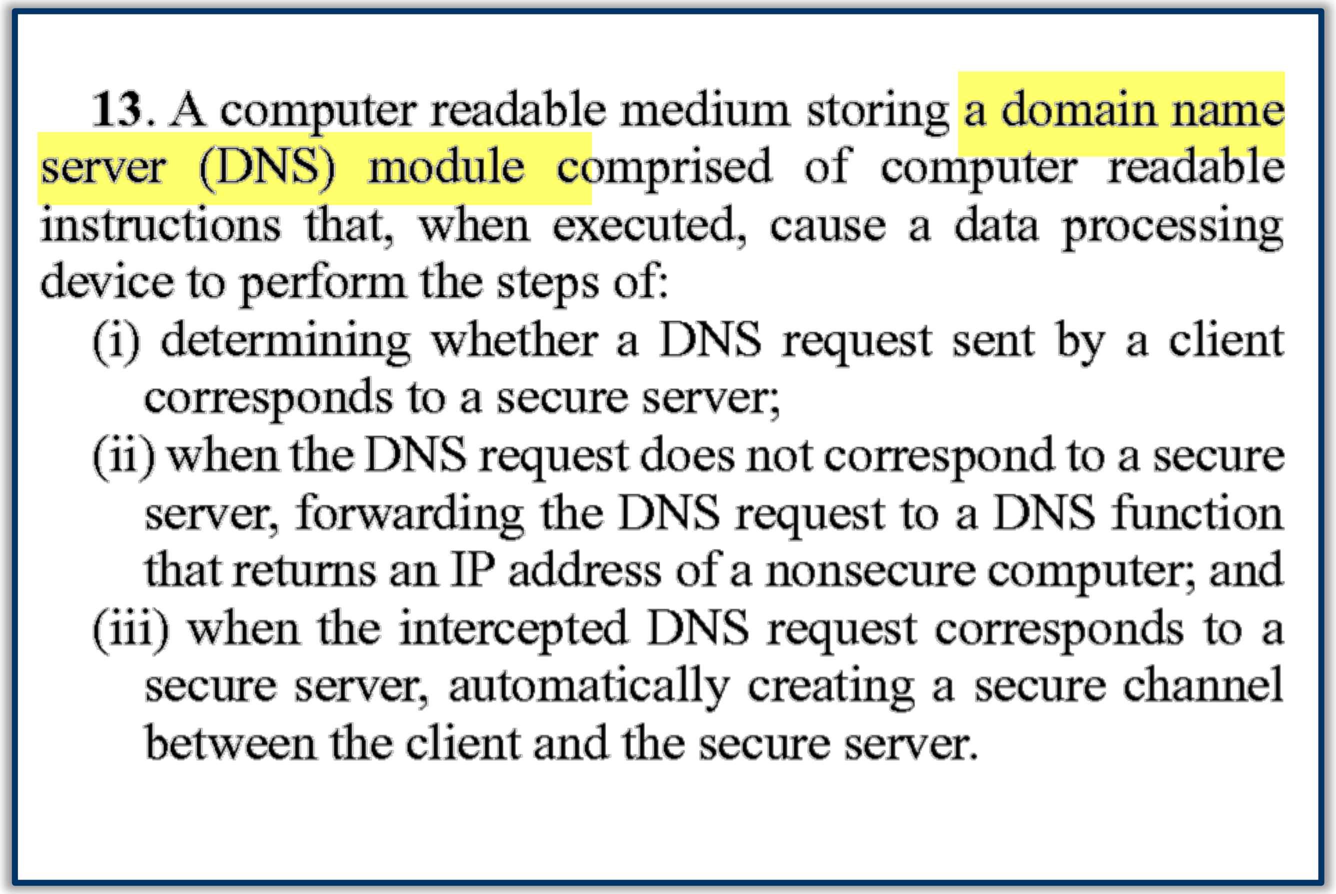


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.

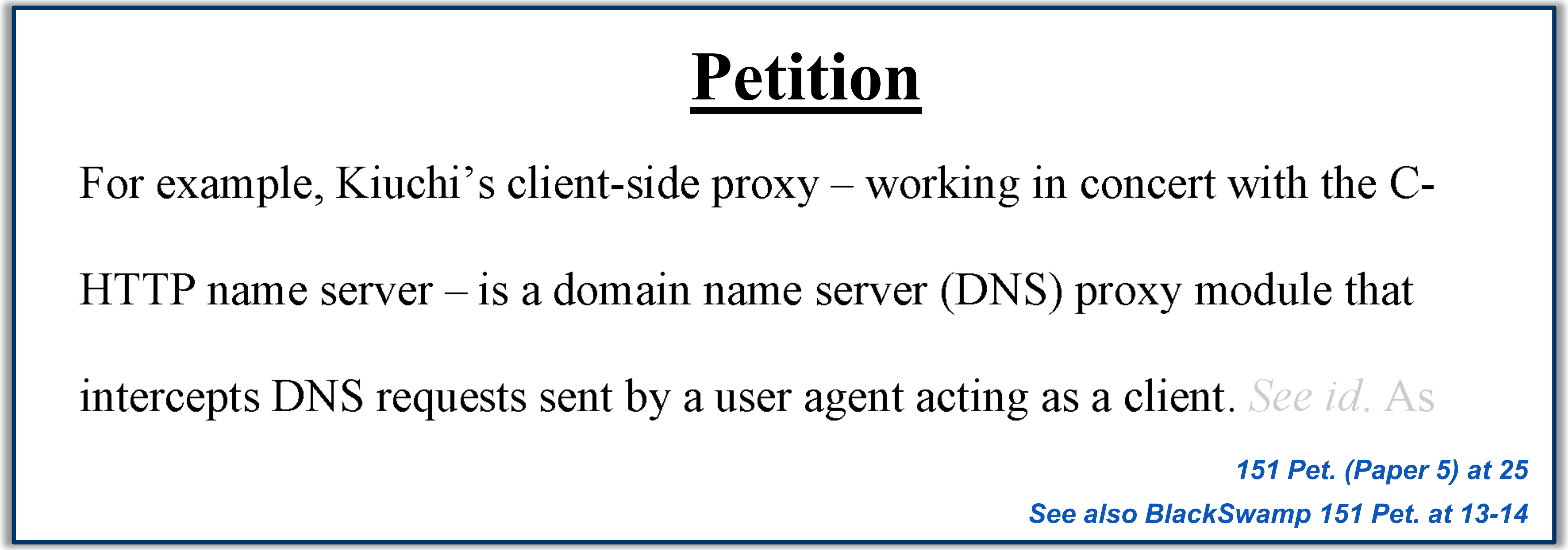


13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.



Petition

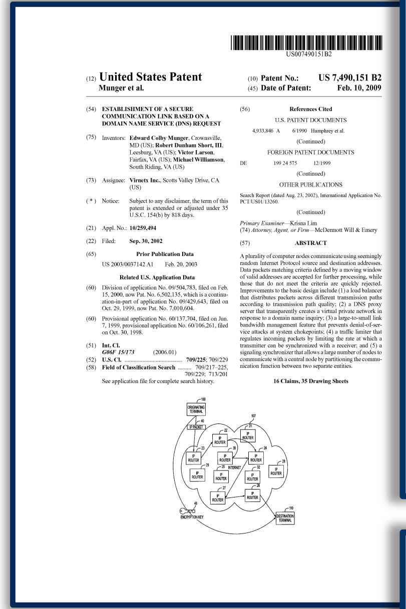
For example, Kiuchi's client-side proxy – working in concert with the C-HTTP name server – is a domain name server (DNS) proxy module that intercepts DNS requests sent by a user agent acting as a client. *See id.* As

151 Pet. (Paper 5) at 25

See also BlackSwamp 151 Pet. at 13-14

The Patent Describes Several DNS Proxy Configurations

151 Patent Ex. 1001



US007490151B2

(12) **United States Patent**
Munger et al.

(10) **Patent No.: US 7,490,151 B2**
(45) **Date of Patent: Feb. 10, 2009**

(54) **ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST**

(75) Inventors: **Edward Colby Munger**, Crownsville, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/259,494**

(22) Filed: **Sep. 30, 2002**

(65) **Prior Publication Data**

US 2003/0037142 A1 Feb. 20, 2003

Related U.S. Application Data

(60) Division 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.** **709/225**; 709/229
(58) **Field of Classification Search** 709/217–225, 709/229; 713/201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A	6/1990	Humphrey et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	199 24 575	12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

(Continued)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emery

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design 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.

16 Claims, 35 Drawing Sheets

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.

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

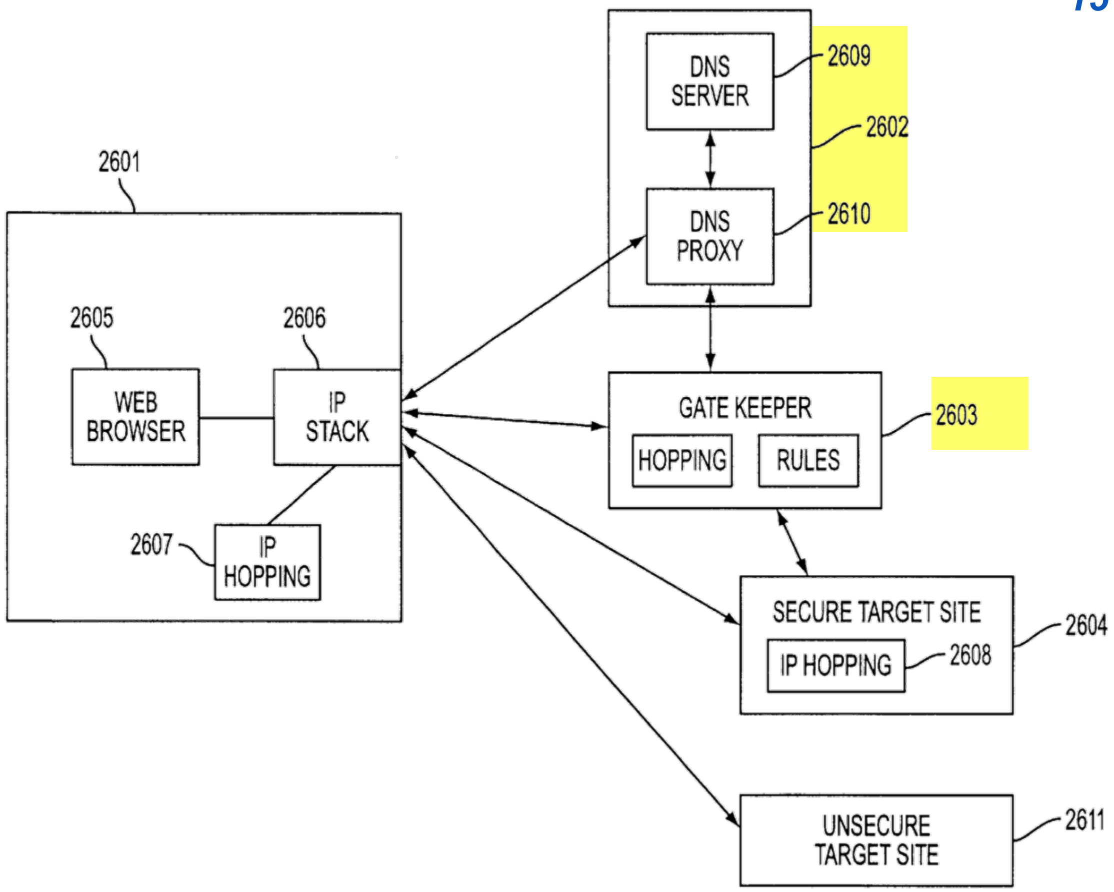
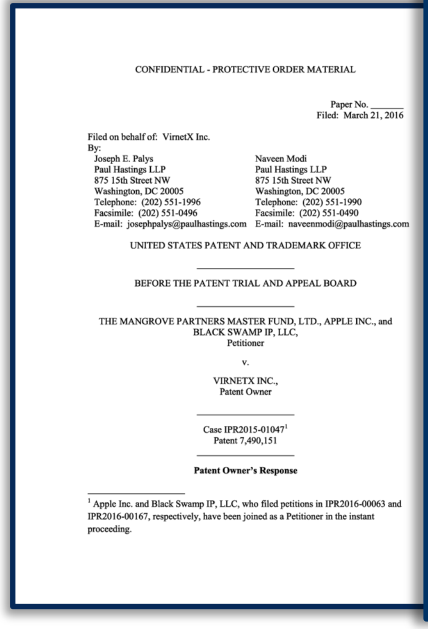


FIG. 26

151 Patent at Fig. 26, 38:22-24, 30-34; Reply at 8-9

Patent Owner: C-HTTP Does Not Follow "DNS" Protocol

Response Paper 48



CONFIDENTIAL - PROTECTIVE ORDER MATERIAL

Paper No. _______
Filed: March 21, 2016

Filed on behalf of: VirnetX Inc.
By:

Joseph E. Palys	Naveen Modi
Paul Hastings LLP	Paul Hastings LLP
875 15th Street NW	875 15th Street NW
Washington, DC 20005	Washington, DC 20005
Telephone: (202) 551-1996	Telephone: (202) 551-1990
Facsimile: (202) 551-0496	Facsimile: (202) 551-0490
E-mail: josephpalys@paulhastings.com	E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD., APPLE INC., and
BLACK SWAMP IP, LLC,
Petitioner

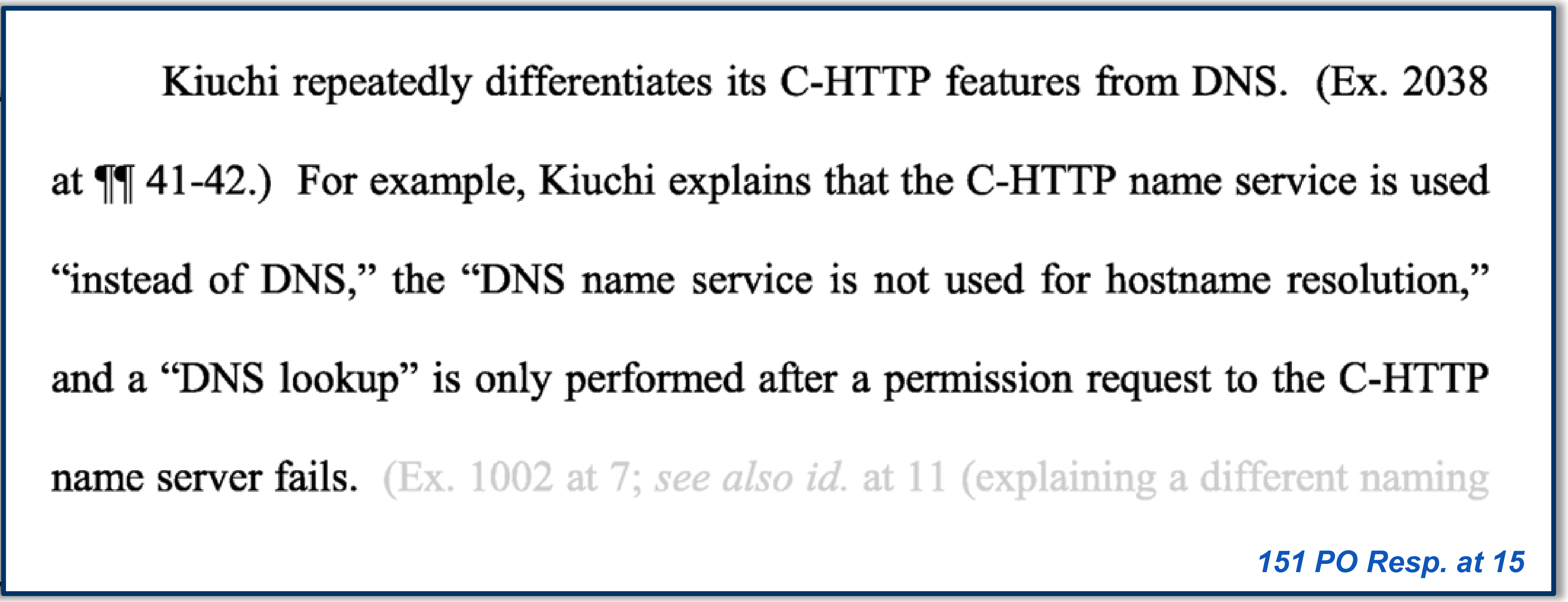
v.

VIRNETX INC.,
Patent Owner

Case IPR2015-01047[1]
Patent 7,490,151

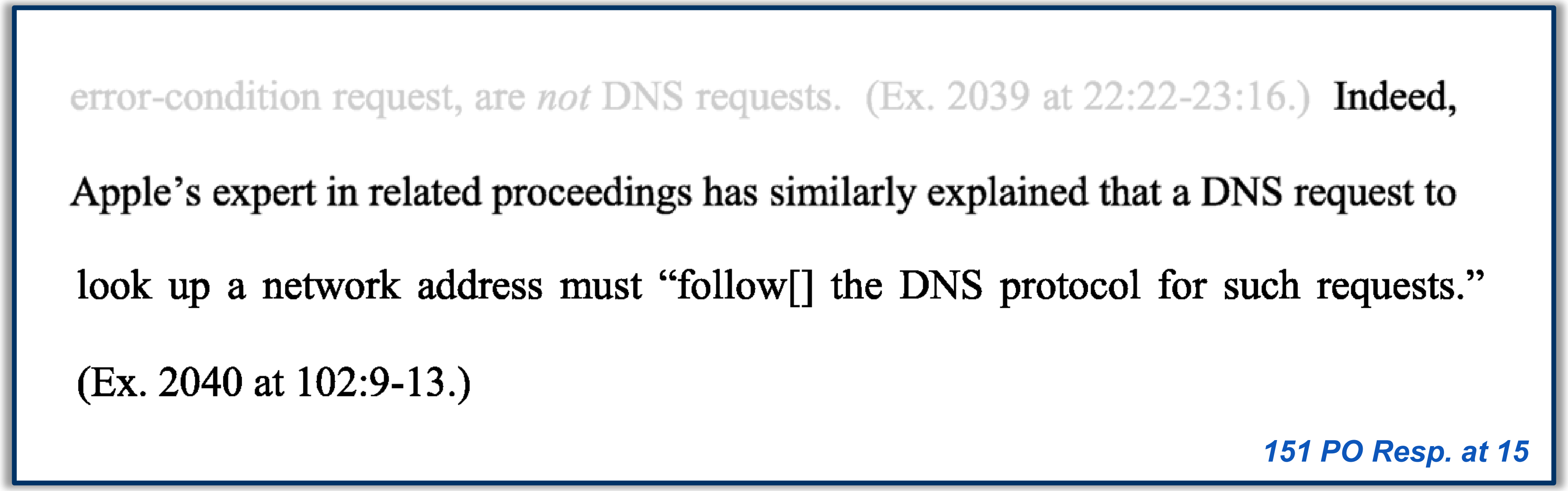
Patent Owner's Response

[1] Apple Inc. and Black Swamp IP, LLC, who filed petitions in IPR2016-00063 and IPR2016-00167, respectively, have been joined as a Petitioner in the instant proceeding.



Kiuchi repeatedly differentiates its C-HTTP features from DNS. (Ex. 2038 at ¶¶ 41-42.) For example, Kiuchi explains that the C-HTTP name service is used "instead of DNS," the "DNS name service is not used for hostname resolution," and a "DNS lookup" is only performed after a permission request to the C-HTTP name server fails. (Ex. 1002 at 7; *see also id.* at 11 (explaining a different naming

151 PO Resp. at 15



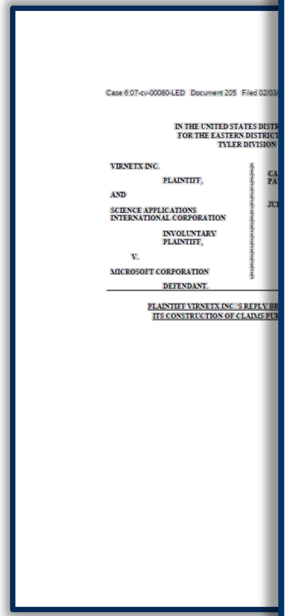
error-condition request, are *not* DNS requests. (Ex. 2039 at 22:22-23:16.) Indeed, Apple's expert in related proceedings has similarly explained that a DNS request to look up a network address must "follow[] the DNS protocol for such requests." (Ex. 2040 at 102:9-13.)

151 PO Resp. at 15

VirnetX: DNS Not Limited to IETF Protocols

Ex. 1038 (VirnetX's District Court Claim Construction Brief) & Ex. 1036 (Dr. Monrose)

VirnetX B
Ex. 10


Case 6:07-cv-00080-LED Document 205 Filed 02/03

IN THE UNITED STATES DISTR
FOR THE EASTERN DISTRICT
TYLER DIVISION

VIRNETX INC.

PLAINTIFF,

AND

SCIENCE APPLICATIONS
INTERNATIONAL CORPORATION

INVOLUNTARY
PLAINTIFF,

V.

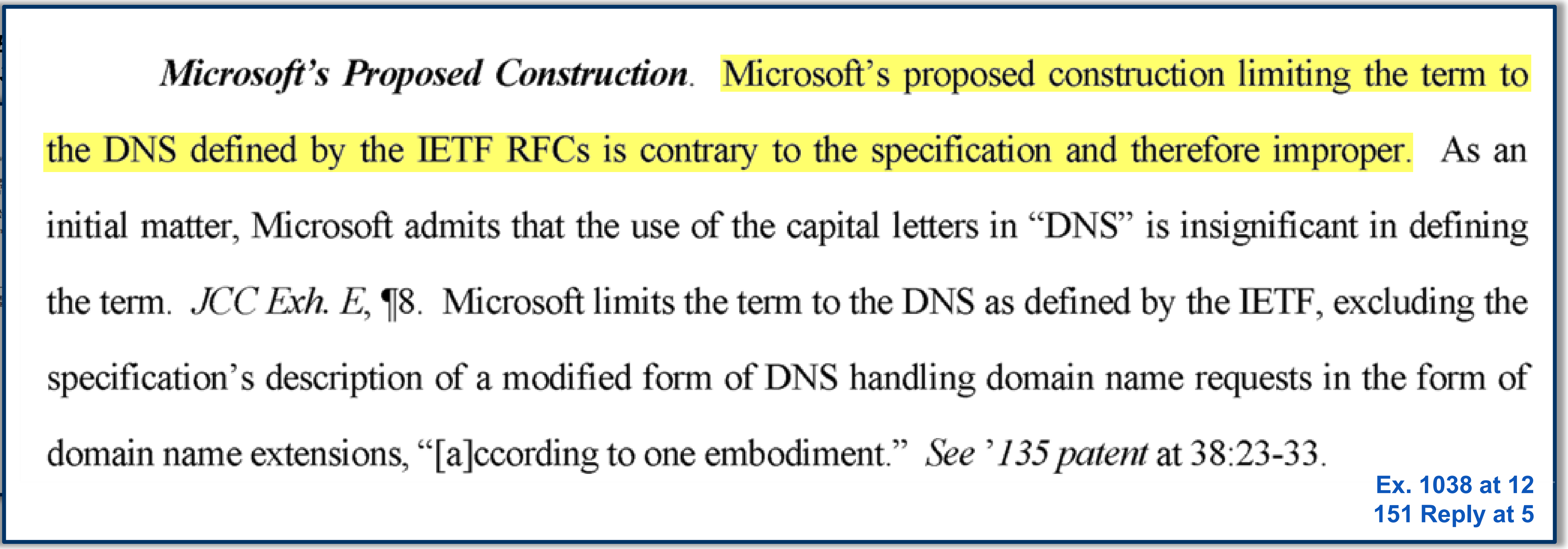
MICROSOFT CORPORATION

DEFENDANT.

CA
PA

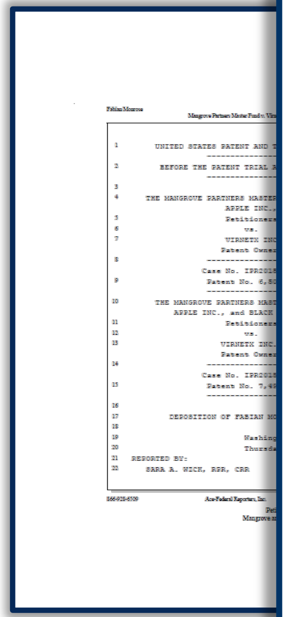
JU

PLAINTIFF VIRNETX INC.'S REPLY BR
ITS CONSTRUCTION OF CLAIMS PUR


Microsoft's Proposed Construction. Microsoft's proposed construction limiting the term to the DNS defined by the IETF RFCs is contrary to the specification and therefore improper. As an initial matter, Microsoft admits that the use of the capital letters in "DNS" is insignificant in defining the term. *JCC Exh. E*, ¶8. Microsoft limits the term to the DNS as defined by the IETF, excluding the specification's description of a modified form of DNS handling domain name requests in the form of domain name extensions, "[a]ccording to one embodiment." *See '135 patent* at 38:23-33.

Ex. 1038 at 12
151 Reply at 5

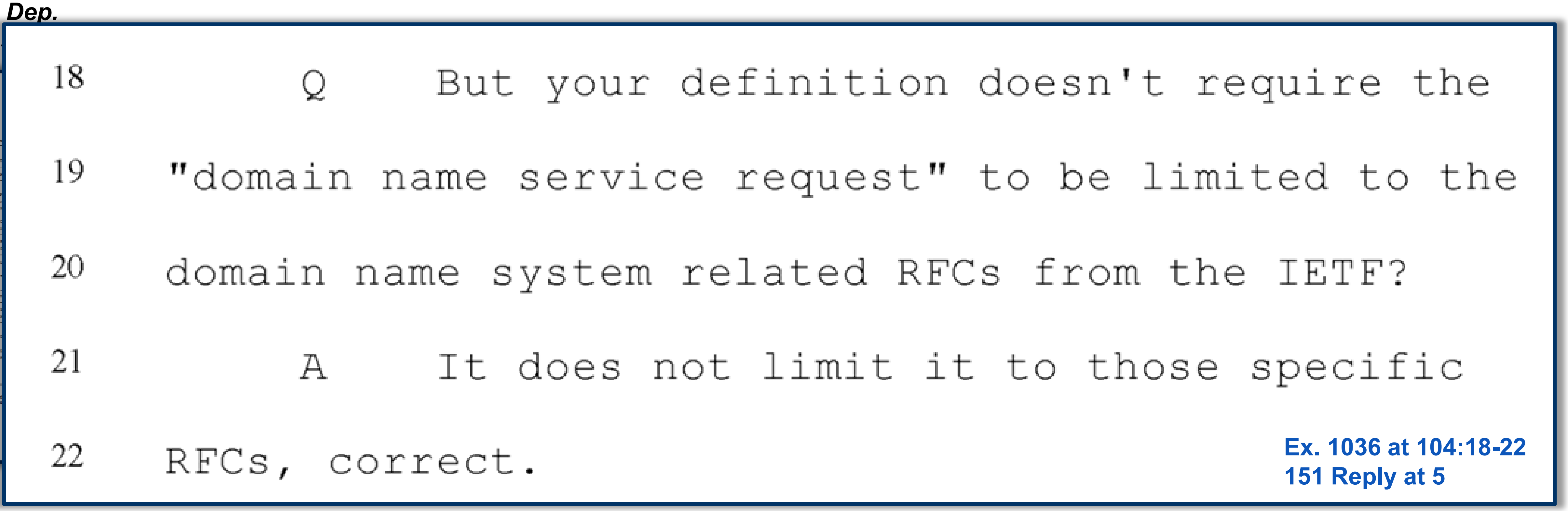
Monrose Dep.
Ex. 10


Fabian Monrose
Mangrove Partners Master Fund v. Vir

UNITED STATES PATENT AND T
BEFORE THE PATENT TRIAL A
THE MANGROVE PARTNERS MASTER
APPLE INC.,
Petitioners
vs.
VIRNETX INC
Patent Owner
Case No. IPR2015
Patent No. 6,50
THE MANGROVE PARTNERS MAST
APPLE INC., and BLACK
Petitioners
vs.
VIRNETX INC.
Patent Owner
Case No. IPR2015
Patent No. 7,49
DEPOSITION OF FABIAN MO
Washing
Thursda
REPORTED BY:
SARA A. WICK, RPR, CRR

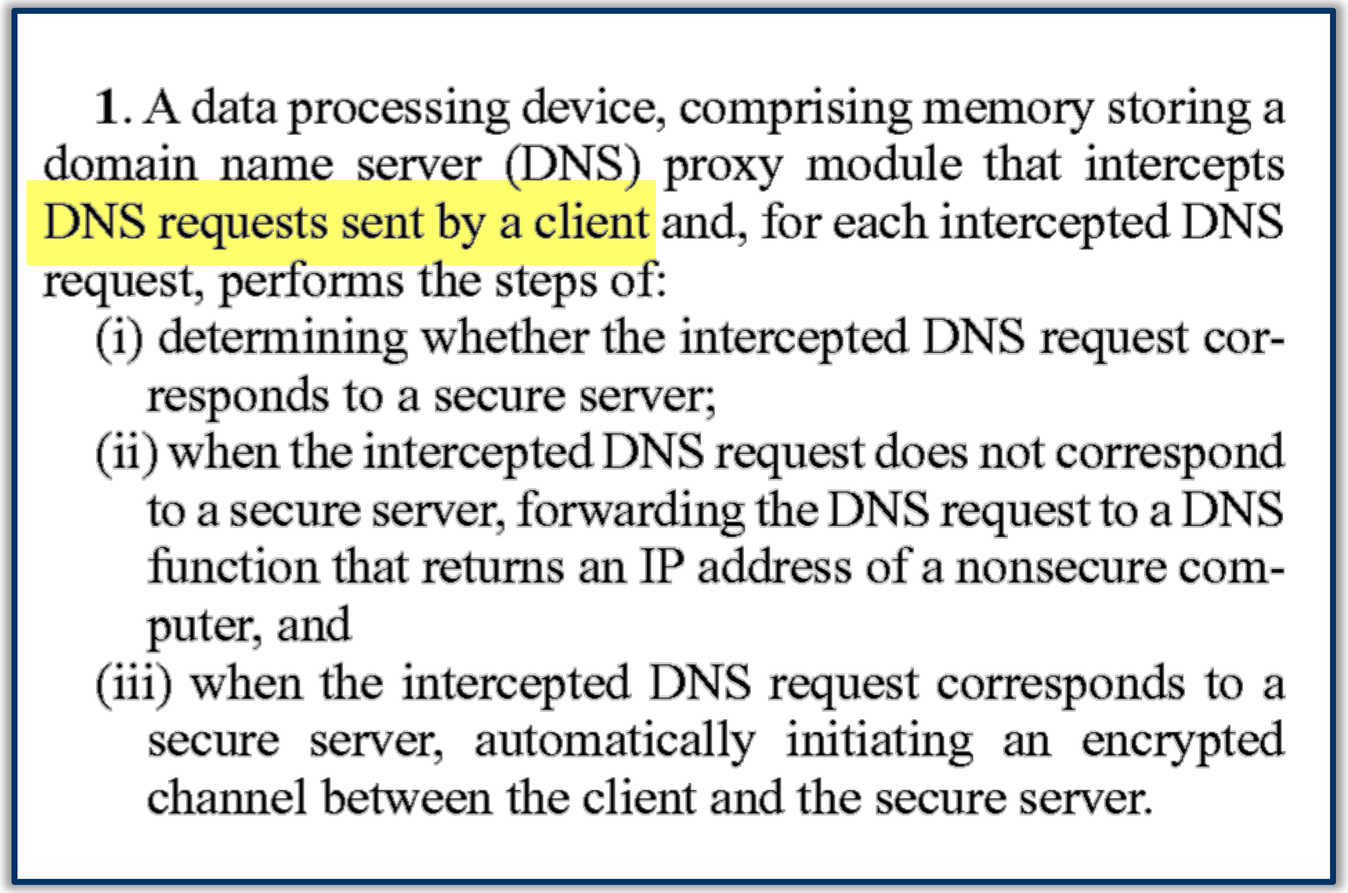
866-928-6509 Ace-Federal Reporters, Inc.

Peti
Mangrove an


```
        Q    But your definition doesn't require the
  "domain name service request" to be limited to the
  domain name system related RFCs from the IETF?
        A    It does not limit it to those specific
  RFCs, correct.
```

Ex. 1036 at 104:18-22
151 Reply at 5

151 Patent

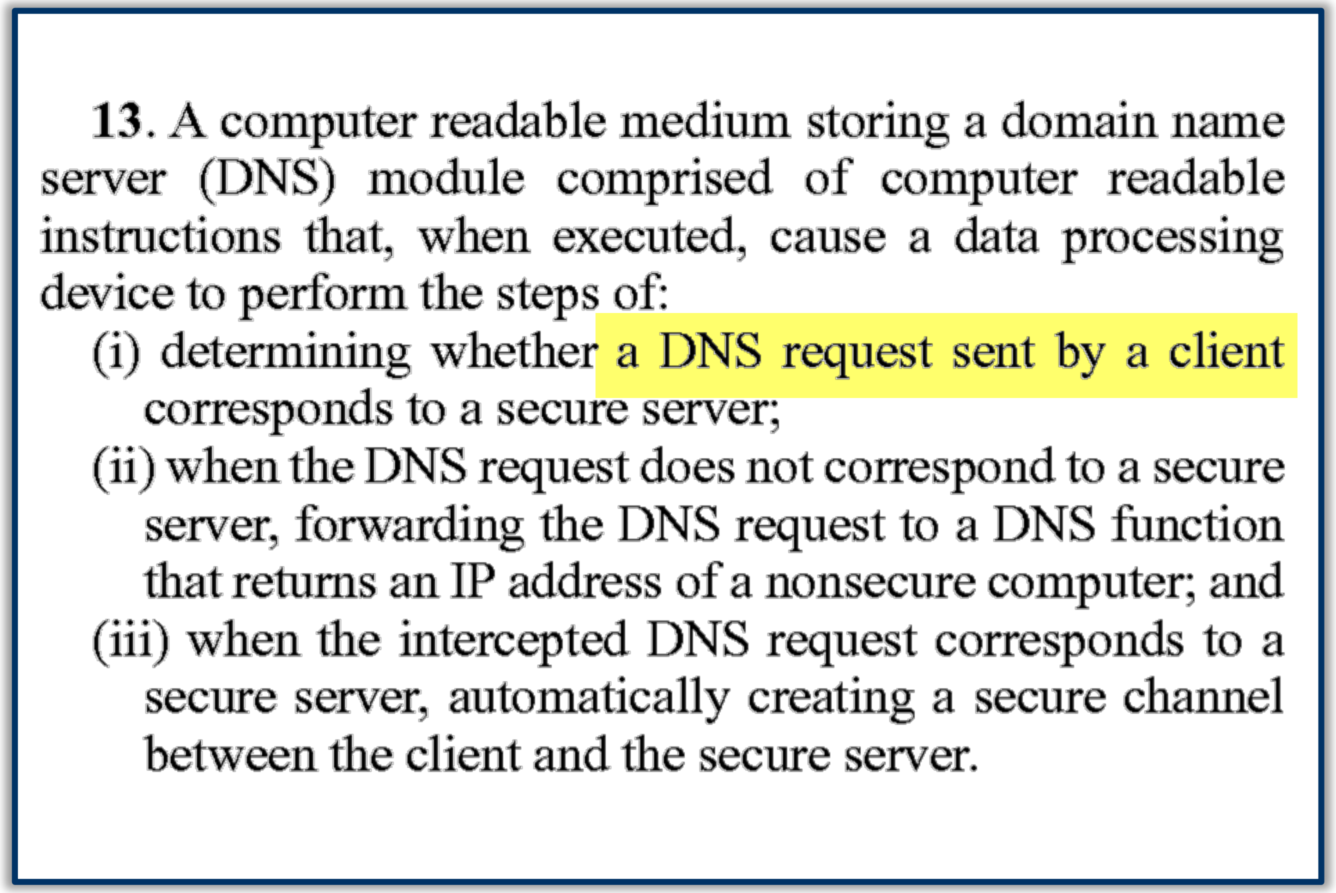


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.



13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

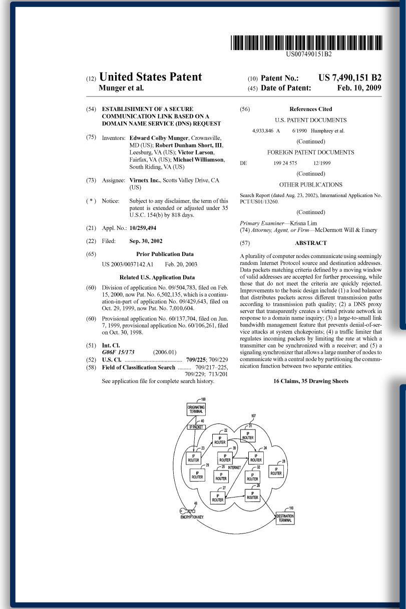
Client

Petitioners' Construction	Patent Owner's Construction
A device, computer, system, or program from which a data request to a server is generated	User's computer

Petition at 15; Resp. at 15

The Patent Describes a “Conventional Client”

151 Patent
Ex. 1001



US007490151B2

(12) **United States Patent**
Munger et al.

(10) **Patent No.:** **US 7,490,151 B2**
(45) **Date of Patent:** **Feb. 10, 2009**

(54) **ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST**

(75) Inventors: **Edward Colby Munger**, Crownsville, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/259,494**

(22) Filed: **Sep. 30, 2002**

(65) **Prior Publication Data**

US 2003/0037142 A1 Feb. 20, 2003

Related U.S. Application Data

(60) Division 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.** **709/225**; 709/229

(58) **Field of Classification Search** 709/217–225, 709/229; 713/201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

(Continued)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emery

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design 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.

16 Claims, 35 Drawing Sheets

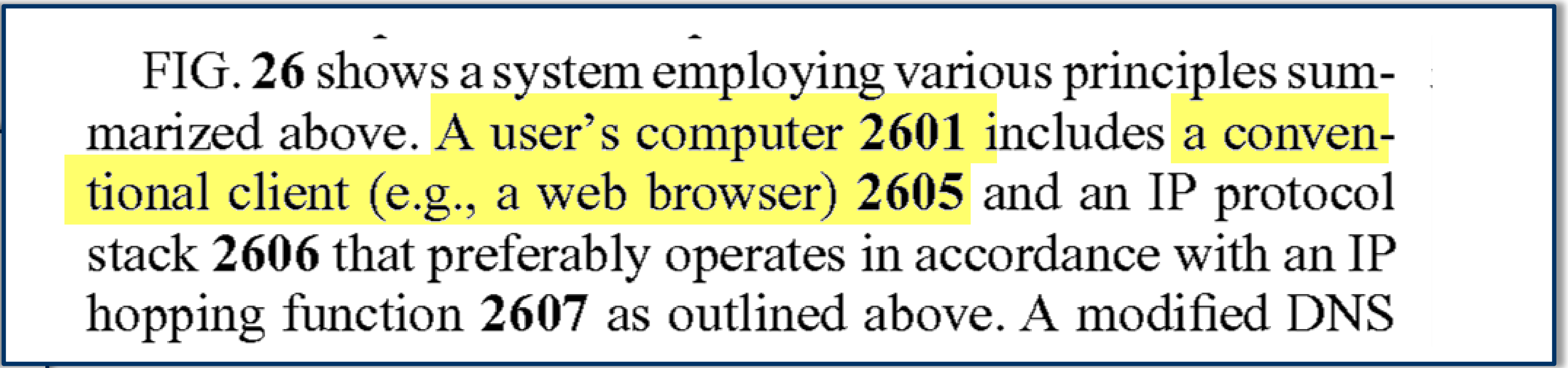


FIG. **26** shows a system employing various principles summarized above. A user’s computer **2601** includes a conventional client (e.g., a web browser) **2605** and an IP protocol stack **2606** that preferably operates in accordance with an IP hopping function **2607** as outlined above. A modified DNS

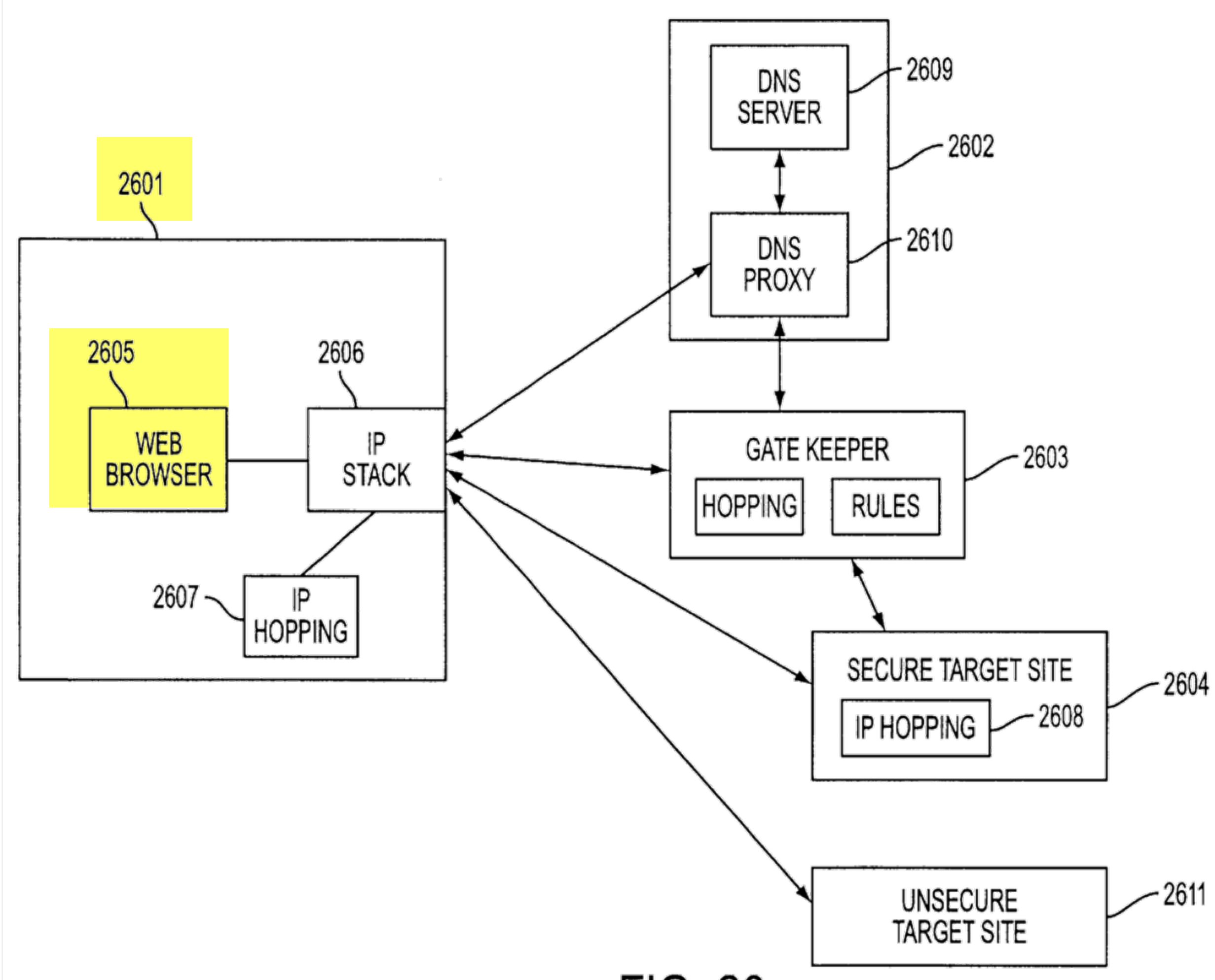


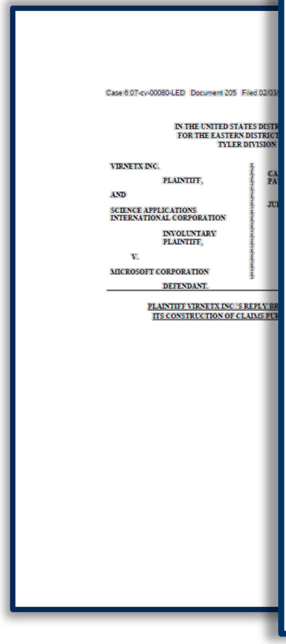
FIG. 26

151 Patent at Fig. 26, 37:50-54;
Reply at 10-11

For ’135 Patent, DNS Proxy Server and Client Can Be on Same Device

Ex. 1038 – Plaintiff VirnetX’s Opening Brief ISO Construction of Claims

VirnetX Brief
Ex. 10

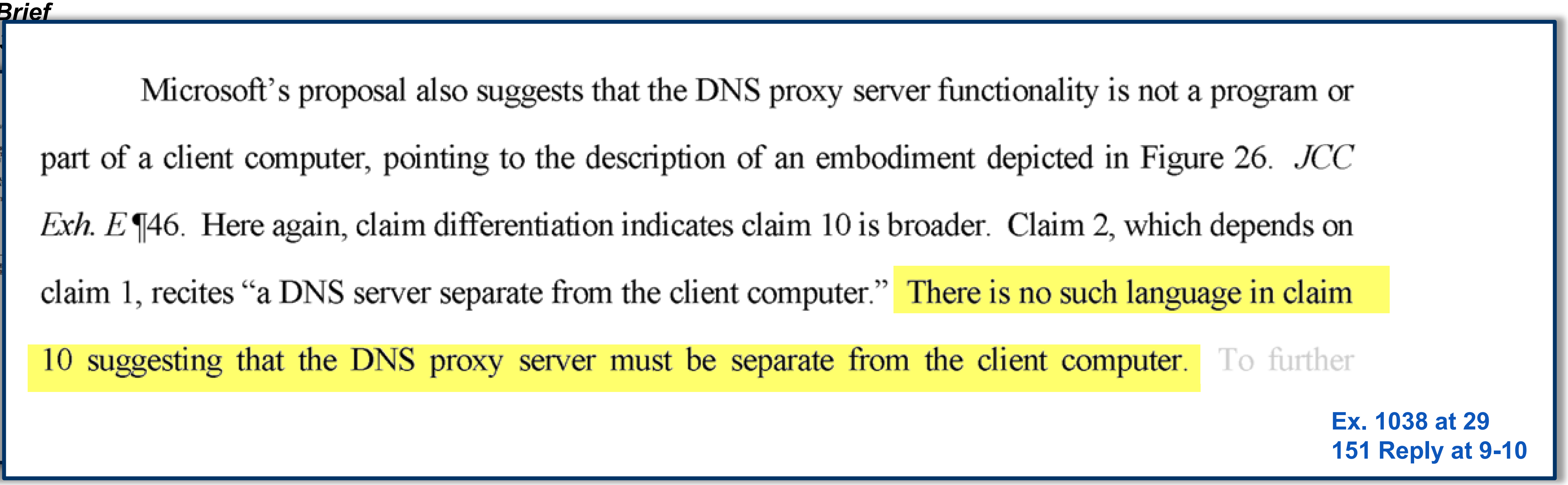


Case 6:07-cv-00080-LED Document 205 Filed 02/03/

IN THE UNITED STATES DISTR
FOR THE EASTERN DISTRICT
TYLER DIVISION

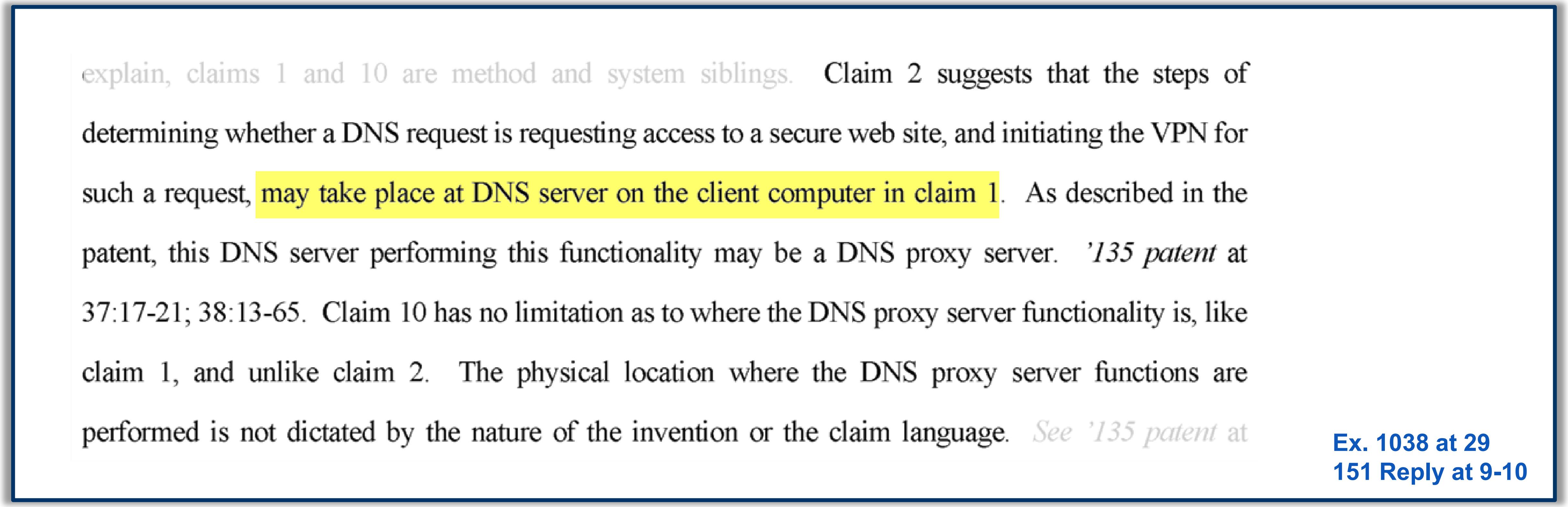
VIRNETX INC. PLAINTIFF, AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION INVOLUNTARY PLAINTIFF, V. MICROSOFT CORPORATION DEFENDANT.	§ § § § § § § § § § § § § §	CA PA JU

PLAINTIFF VIRNETX INC.'S REPLY BR
ITS CONSTRUCTION OF CLAIMS PUR



Microsoft’s proposal also suggests that the DNS proxy server functionality is not a program or part of a client computer, pointing to the description of an embodiment depicted in Figure 26. *JCC Exh. E* ¶46. Here again, claim differentiation indicates claim 10 is broader. Claim 2, which depends on claim 1, recites “a DNS server separate from the client computer.” There is no such language in claim 10 suggesting that the DNS proxy server must be separate from the client computer. To further

Ex. 1038 at 29
151 Reply at 9-10

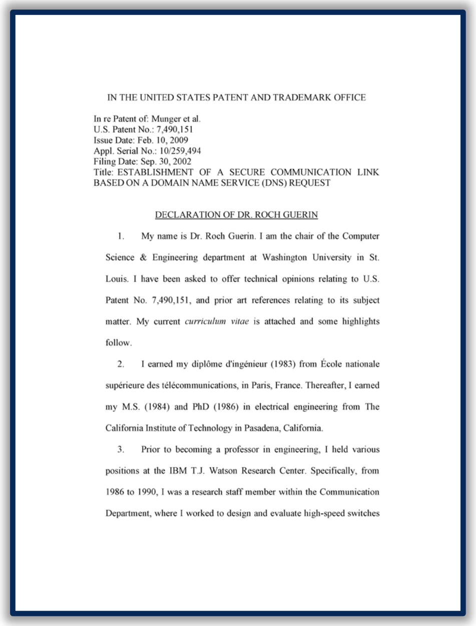


explain, claims 1 and 10 are method and system siblings. Claim 2 suggests that the steps of determining whether a DNS request is requesting access to a secure web site, and initiating the VPN for such a request, may take place at DNS server on the client computer in claim 1. As described in the patent, this DNS server performing this functionality may be a DNS proxy server. *’135 patent* at 37:17-21; 38:13-65. Claim 10 has no limitation as to where the DNS proxy server functionality is, like claim 1, and unlike claim 2. The physical location where the DNS proxy server functions are performed is not dictated by the nature of the invention or the claim language. *See ’135 patent* at

Ex. 1038 at 29
151 Reply at 9-10

Dr. Guerin: A “Client” Makes Requests

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 7,490,151
Issue Date: Feb. 10, 2009
Appl. Serial No.: 10/259,494
Filing Date: Sep. 30, 2002
Title: ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST

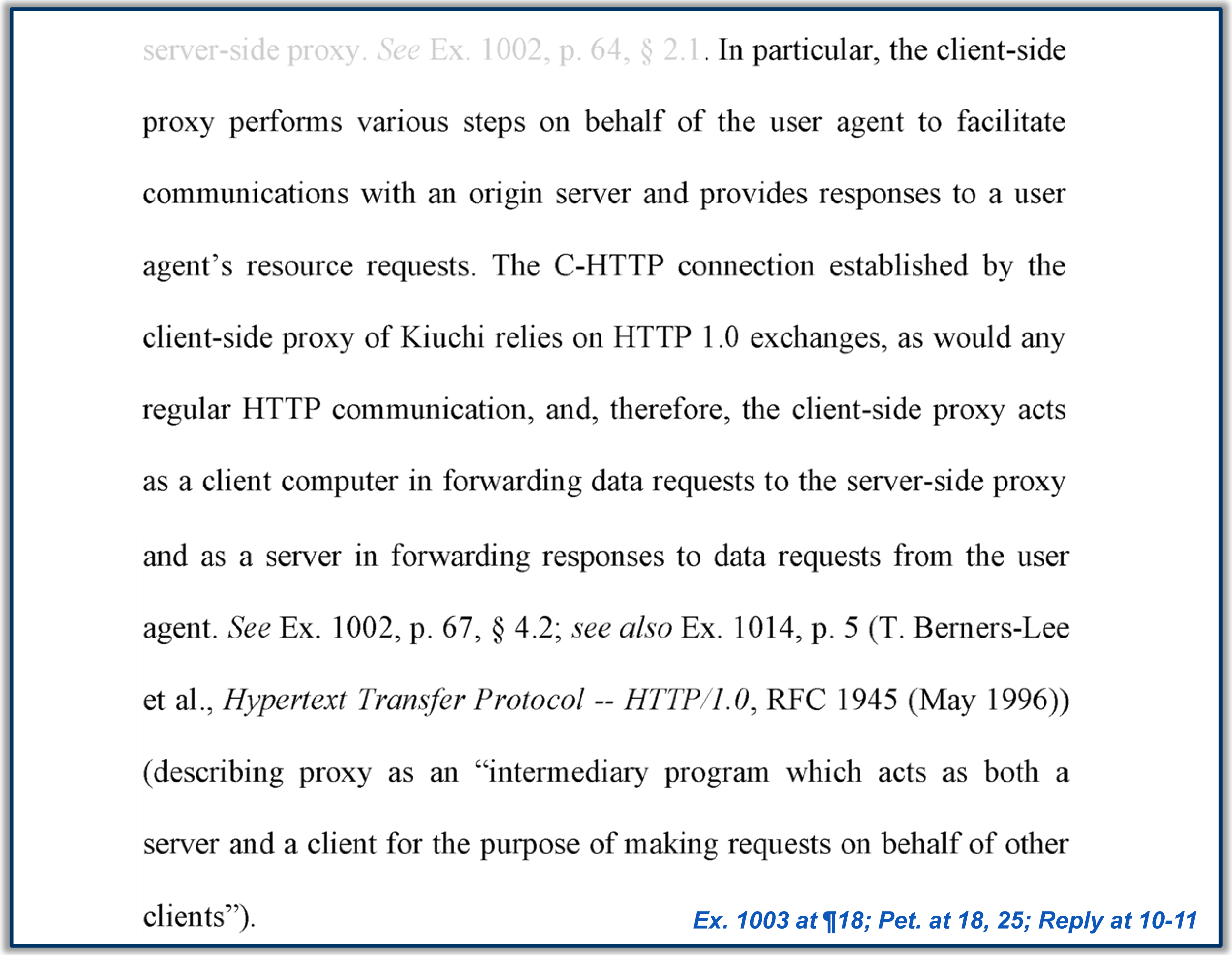
DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Science & Engineering department at Washington University in St. Louis. I have been asked to offer technical opinions relating to U.S. Patent No. 7,490,151, and prior art references relating to its subject matter. My current *curriculum vitae* is attached and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure des télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) and PhD (1986) in electrical engineering from The California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at the IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I was a research staff member within the Communication Department, where I worked to design and evaluate high-speed switches

Dr. Guerin

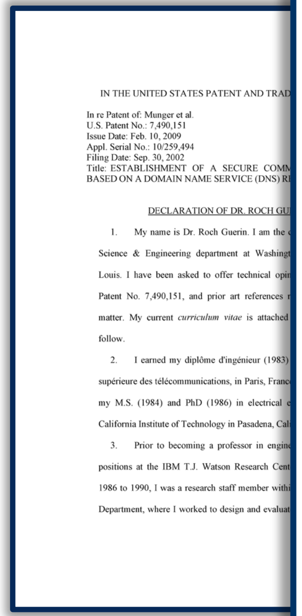


server-side proxy. *See* Ex. 1002, p. 64, § 2.1. In particular, the client-side proxy performs various steps on behalf of the user agent to facilitate communications with an origin server and provides responses to a user agent’s resource requests. The C-HTTP connection established by the client-side proxy of Kiuchi relies on HTTP 1.0 exchanges, as would any regular HTTP communication, and, therefore, the client-side proxy acts as a client computer in forwarding data requests to the server-side proxy and as a server in forwarding responses to data requests from the user agent. *See* Ex. 1002, p. 67, § 4.2; *see also* Ex. 1014, p. 5 (T. Berners-Lee et al., *Hypertext Transfer Protocol -- HTTP/1.0*, RFC 1945 (May 1996)) (describing proxy as an “intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients”).

Ex. 1003 at ¶18; Pet. at 18, 25; Reply at 10-11

Dr. Guerin: A “Client” Makes Requests

Dr. Gue
Ex. 10



IN THE UNITED STATES PATENT AND TRAD

In re Patent of: Munger et al.
U.S. Patent No.: 7,490,151
Issue Date: Feb. 10, 2009
Appl. Serial No.: 10/259,494
Filing Date: Sep. 30, 2002
Title: ESTABLISHMENT OF A SECURE COMM
BASED ON A DOMAIN NAME SERVICE (DNS) R

DECLARATION OF DR. ROCH GU

1. My name is Dr. Roch Guerin. I am the
Science & Engineering department at Washingt
Louis. I have been asked to offer technical opi
Patent No. 7,490,151, and prior art references
matter. My current *curriculum vitae* is attached
follow.

2. I earned my diplôme d'ingénieur (1983)
supérieure des télécommunications, in Paris, Franc
my M.S. (1984) and PhD (1986) in electrical
California Institute of Technology in Pasadena, Cal

3. Prior to becoming a professor in engine
positions at the IBM T.J. Watson Research Cent
1986 to 1990, I was a research staff member with
Department, where I worked to design and evalua

RFC 1945

client

An application program that establishes connections for the purpose of sending requests.

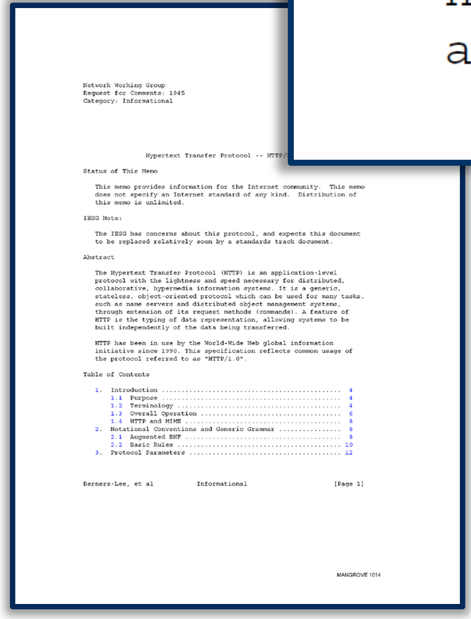
proxy

An intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them, with possible translation, on to other servers. A proxy must interpret and, if necessary, rewrite a request message before forwarding it. Proxies are often used as client-side portals through network firewalls and as helper applications for handling requests via protocols not implemented by the user agent.

Ex. 1014 at 5-6

agent. *See* Ex. 1002, p. 67, § 4.2; *see also* Ex. 1014, p. 5 (T. Berners-Lee et al., *Hypertext Transfer Protocol -- HTTP/1.0*, RFC 1945 (May 1996)) (describing proxy as an “intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients”).

Ex. 1003 at ¶18; Pet. at 18, 25; Reply at 10-11



Network Working Group
Request for Comments: 1945
Category: Informational

Hypertext Transfer Protocol -- HTTP/

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

IESG Note:

The IESG has concerns about this protocol, and expects this document to be replaced relatively soon by a standards track document.

Abstract

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol which can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods (commands). A feature of HTTP is the typing of data representation, allowing systems to be built independently of the data being transferred.

HTTP has been in use by the World-Wide Web global information initiative since 1990. This specification reflects common usage of the protocol referred to as "HTTP/1.0".

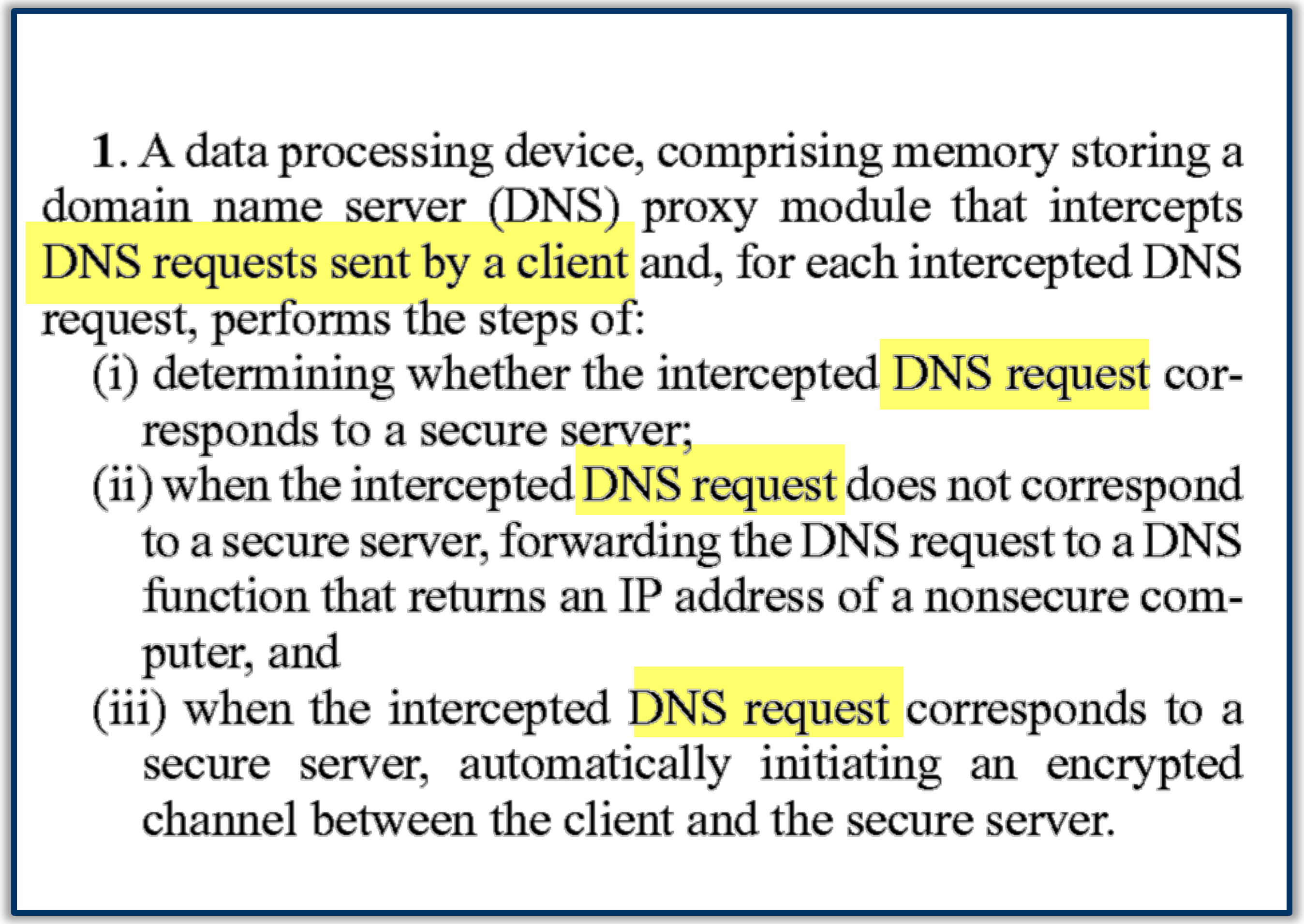
Table of Contents

Berners-Lee, et al   Informational   [Page 1]

MANGROVE 1014

RFC 1945
Ex. 1014

151 Patent

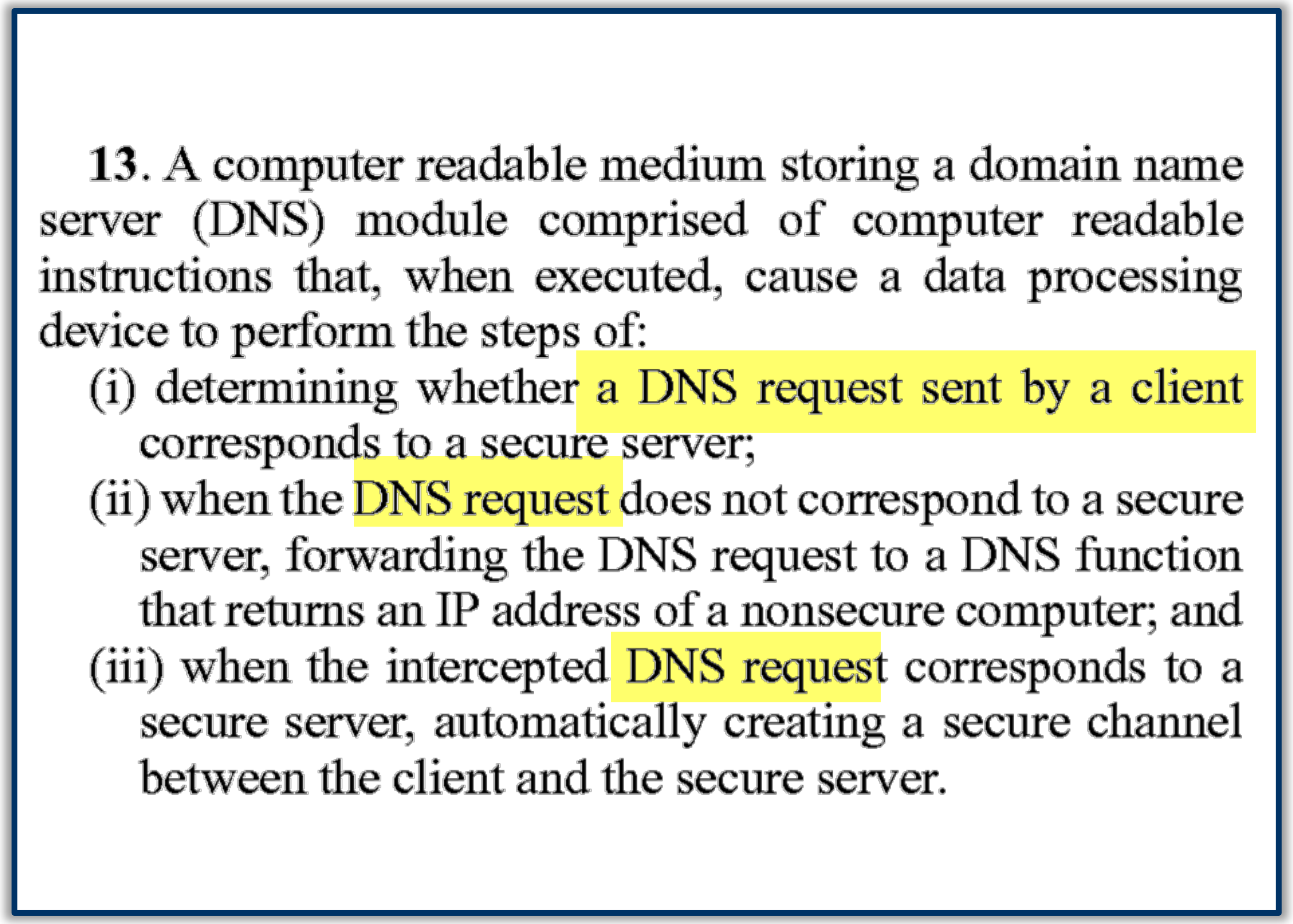


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.



13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

DNS Request

Mangrove's and Apple's Construction	Patent Owner's and Black Swamp's Construction
A request for a resource corresponding to a network address	A request for a resource corresponding to a domain name

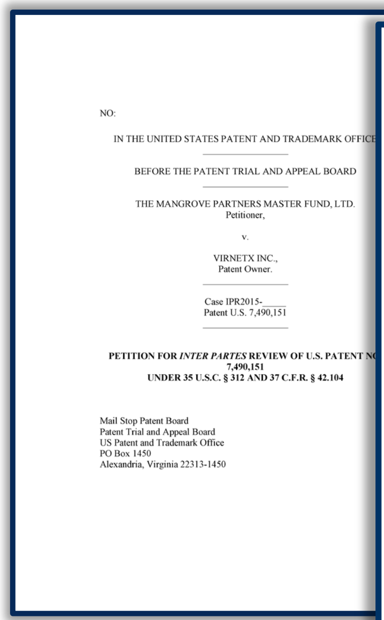
151 Petition at 9; Resp. at 13

Kiuchi

“a DNS request sent by a client”

Petition

Petition Paper 5



NO:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD.
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-_____
Patent U.S. 7,490,151

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO
7,490,151
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

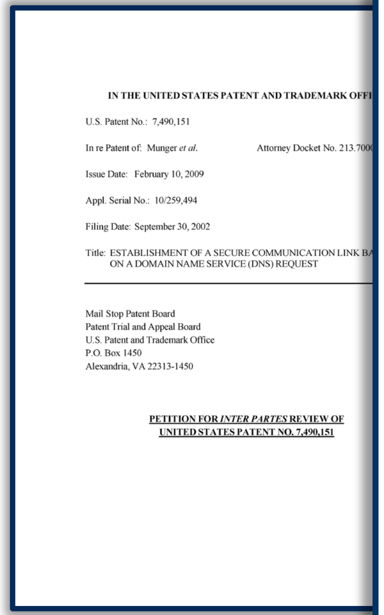
Mail Stop Patent Board
Patent Trial and Appeal Board
US Patent and Trademark Office
PO Box 1450
Alexandria, Virginia 22313-1450

from which a data request to a server is generated. The request from the user agent sent to the client-side proxy is a “DNS request,” under that term’s broadest reasonable interpretation, because the request is a request for a resource (e.g., an HTML document) corresponding to a domain name (the hostname).

151 Pet. (Paper 5) at 26

is “6zdDfldfcZLj8V!i.” Accordingly, the user agent’s request is necessarily a request for a resource corresponding to a hostname in a hyperlink URL. (See Kiuchi (Ex. 1004) at page 65, § 2.3.) Furthermore, the request from the client-side proxy is necessarily a request for resources corresponding to the hostname. (Kiuchi (Ex. 1004) at page 65, § 2.3.)

BlackSwamp 151 Pet. (Paper 1) at 14



IN THE UNITED STATES PATENT AND TRADEMARK OFFI

U.S. Patent No.: 7,490,151

In re Patent of: Munger *et al.* Attorney Docket No. 213.7000

Issue Date: February 10, 2009

Appl. Serial No.: 10/259,494

Filing Date: September 30, 2002

Title: ESTABLISHMENT OF A SECURE COMMUNICATION LINK BA
ON A DOMAIN NAME SERVICE (DNS) REQUEST

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

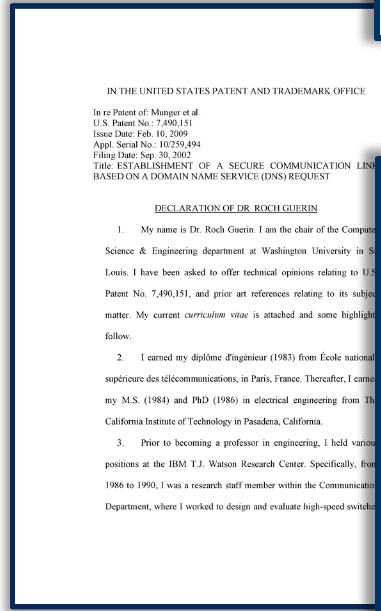
**PETITION FOR *INTER PARTES* REVIEW OF
UNITED STATES PATENT NO. 7,490,151**

***Black Swamp
IPR2016-00167, Paper 1***

Kiuchi

"a DNS request sent by a client"

Dr. Guerin Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 7,490,151
Issue Date: Feb. 10, 2009
Appl. Serial No.: 10/259,494
Filing Date: Sep. 30, 2002
Title: ESTABLISHMENT OF A SECURE COMMUNICATION LIN
BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST

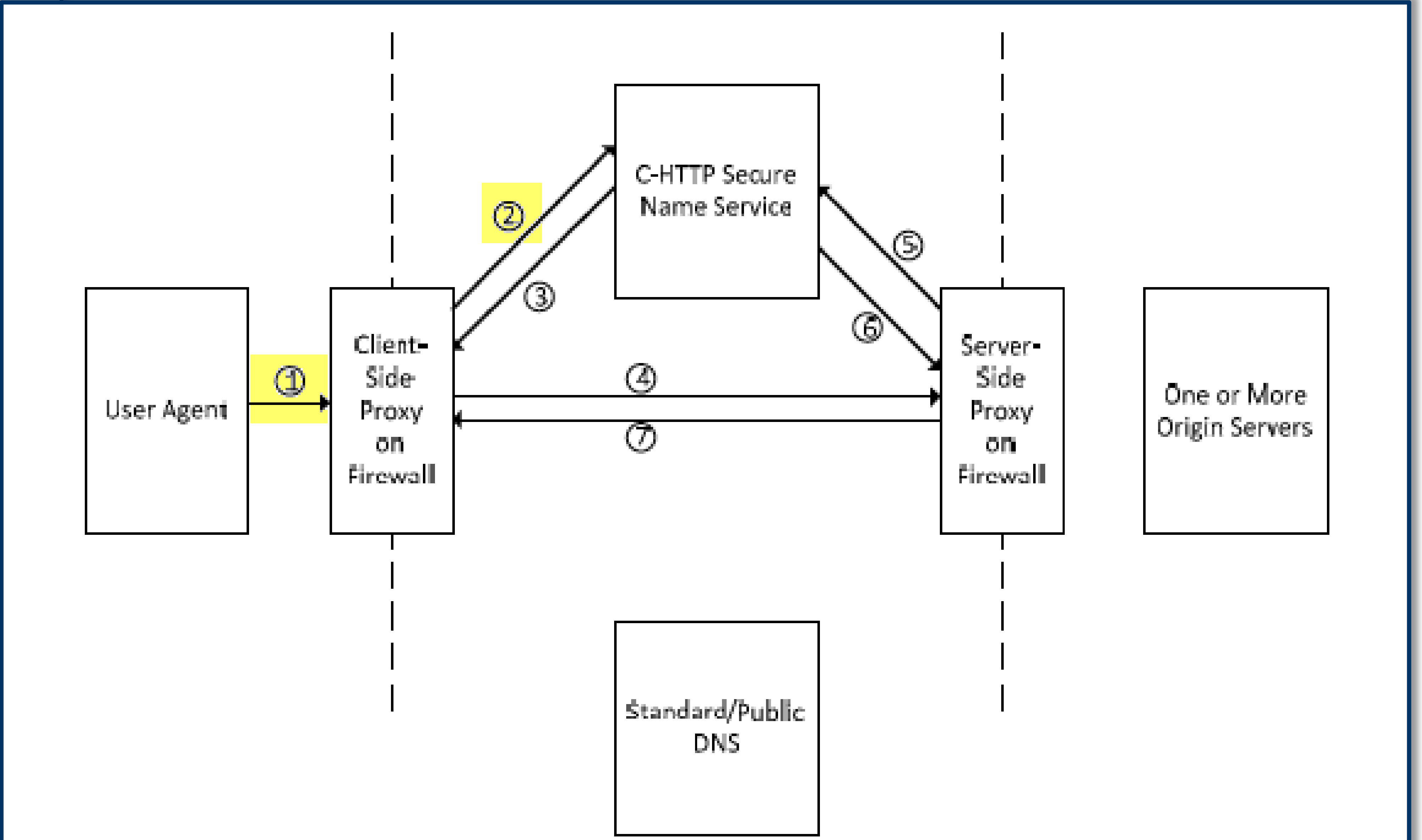
DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Compute
Science & Engineering department at Washington University in S
Louis. I have been asked to offer technical opinions relating to U.S
Patent No. 7,490,151, and prior art references relating to its subje
matter. My current *curriculum vitae* is attached and some highlight
follow.

2. I earned my diplôme d'ingénieur (1983) from École national
supérieure des télécommunications, in Paris, France. Thereafter, I earne
my M.S. (1984) and PhD (1986) in electrical engineering from Th
California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held variou
positions at the IBM T.J. Watson Research Center. Specifically, fro
1986 to 1990, I was a research staff member within the Communicatio
Department, where I worked to design and evaluate high-speed switche

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



C-HTTP Secure Name Service
②
③
⑤
⑥
User Agent
①
Client-Side Proxy on Firewall
④
⑦
Server-Side Proxy on Firewall
One or More Origin Servers
Standard/Public DNS

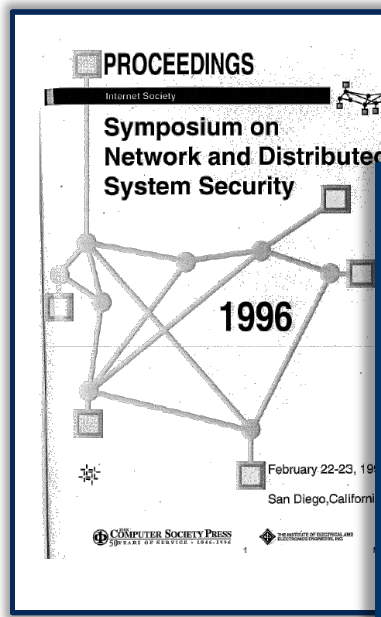
Diagram 2

151 Pet. (Paper 5) at 19; Ex. 1003 at ¶19

Kiuchi

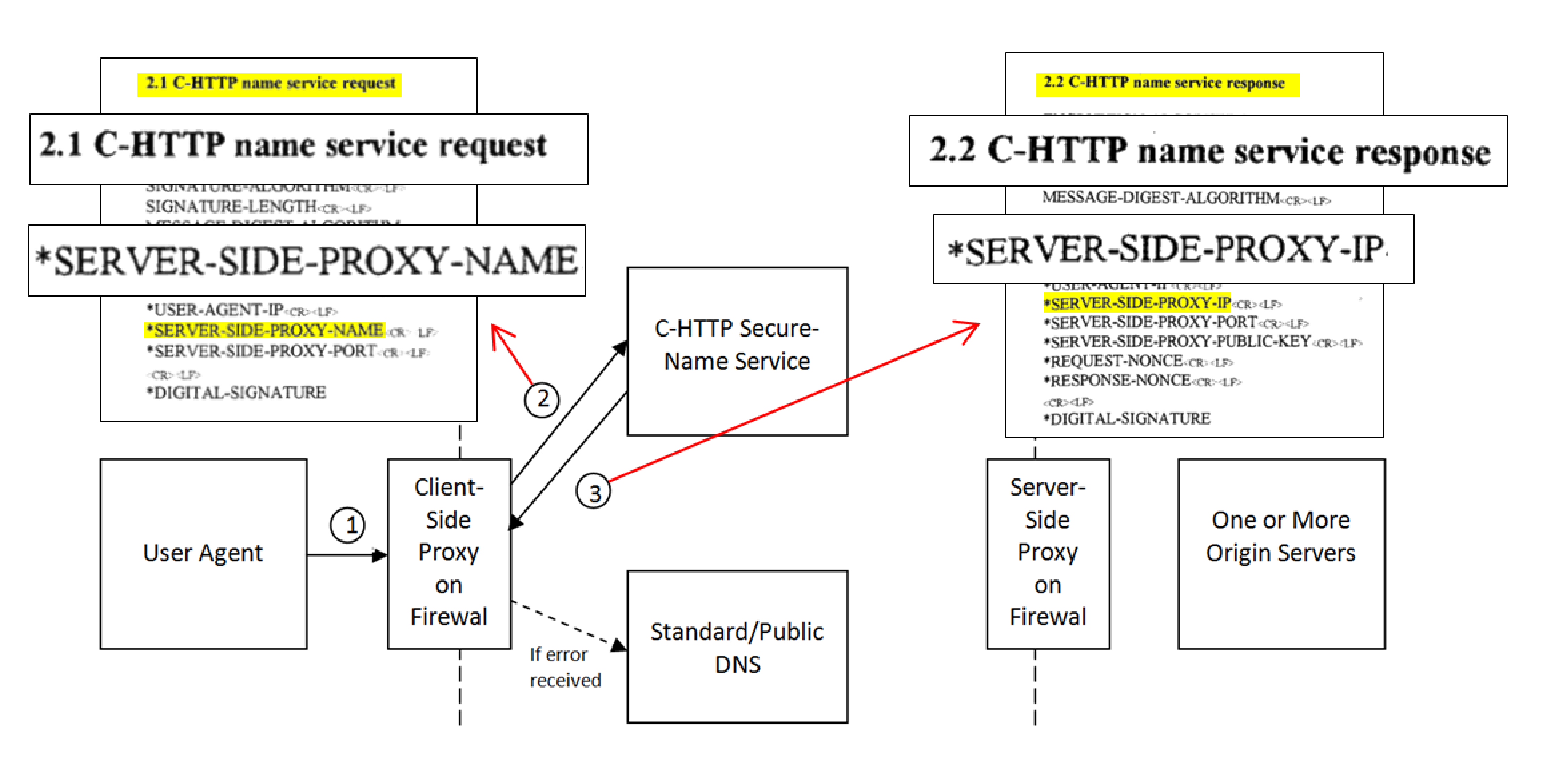
"a DNS request sent by a client"

Kiuchi
Ex. 1002



PROCEEDINGS
Internet Society
Symposium on Network and Distributed System Security
1996
February 22-23, 19
San Diego, Californi
COMPUTER SOCIETY PRESS

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



2.1 C-HTTP name service request

2.1 C-HTTP name service request

SIGNATURE-ALGORITHM<CR><LF>
SIGNATURE-LENGTH<CR><LF>
MESSAGE-DIGEST-ALGORITHM

***SERVER-SIDE-PROXY-NAME**

*USER-AGENT-IP<CR><LF>
*SERVER-SIDE-PROXY-NAME<CR><LF>
*SERVER-SIDE-PROXY-PORT<CR><LF>
<CR><LF>
*DIGITAL-SIGNATURE

2.2 C-HTTP name service response

2.2 C-HTTP name service response

MESSAGE-DIGEST-ALGORITHM<CR><LF>

***SERVER-SIDE-PROXY-IP**

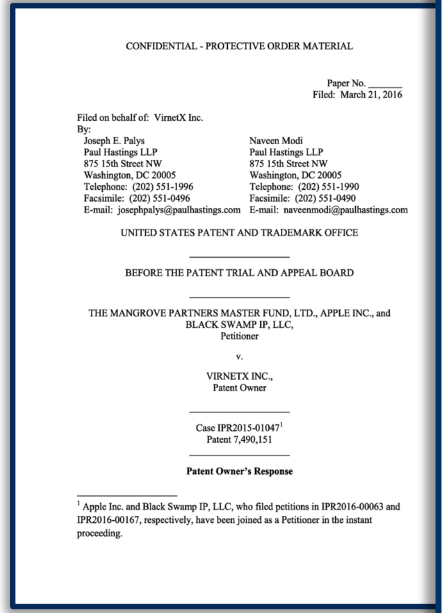
*USER-AGENT-IP<CR><LF>
*SERVER-SIDE-PROXY-IP<CR><LF>
*SERVER-SIDE-PROXY-PORT<CR><LF>
*SERVER-SIDE-PROXY-PUBLIC-KEY<CR><LF>
*REQUEST-NONCE<CR><LF>
*RESPONSE-NONCE<CR><LF>
<CR><LF>
*DIGITAL-SIGNATURE

User Agent
1
Client-Side Proxy on Firewal
2
3
C-HTTP Secure-Name Service
If error received
Standard/Public DNS
Server-Side Proxy on Firewal
One or More Origin Servers

151 Reply at 7

VirnetX: C-HTTP Name Server Does Not Return the Address "Corresponding" to the Domain Name

Response Paper 48



CONFIDENTIAL - PROTECTIVE ORDER MATERIAL

Paper No. ________
Filed: March 21, 2016

Filed on behalf of: VirnetX Inc.
By:

Joseph E. Palys	Naveen Modi
Paul Hastings LLP	Paul Hastings LLP
875 15th Street NW	875 15th Street NW
Washington, DC 20005	Washington, DC 20005
Telephone: (202) 551-1996	Telephone: (202) 551-1990
Facsimile: (202) 551-0496	Facsimile: (202) 551-0490
E-mail: josephpalys@paulhastings.com	E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD., APPLE INC., and
BLACK SWAMP IP, LLC,
Petitioner

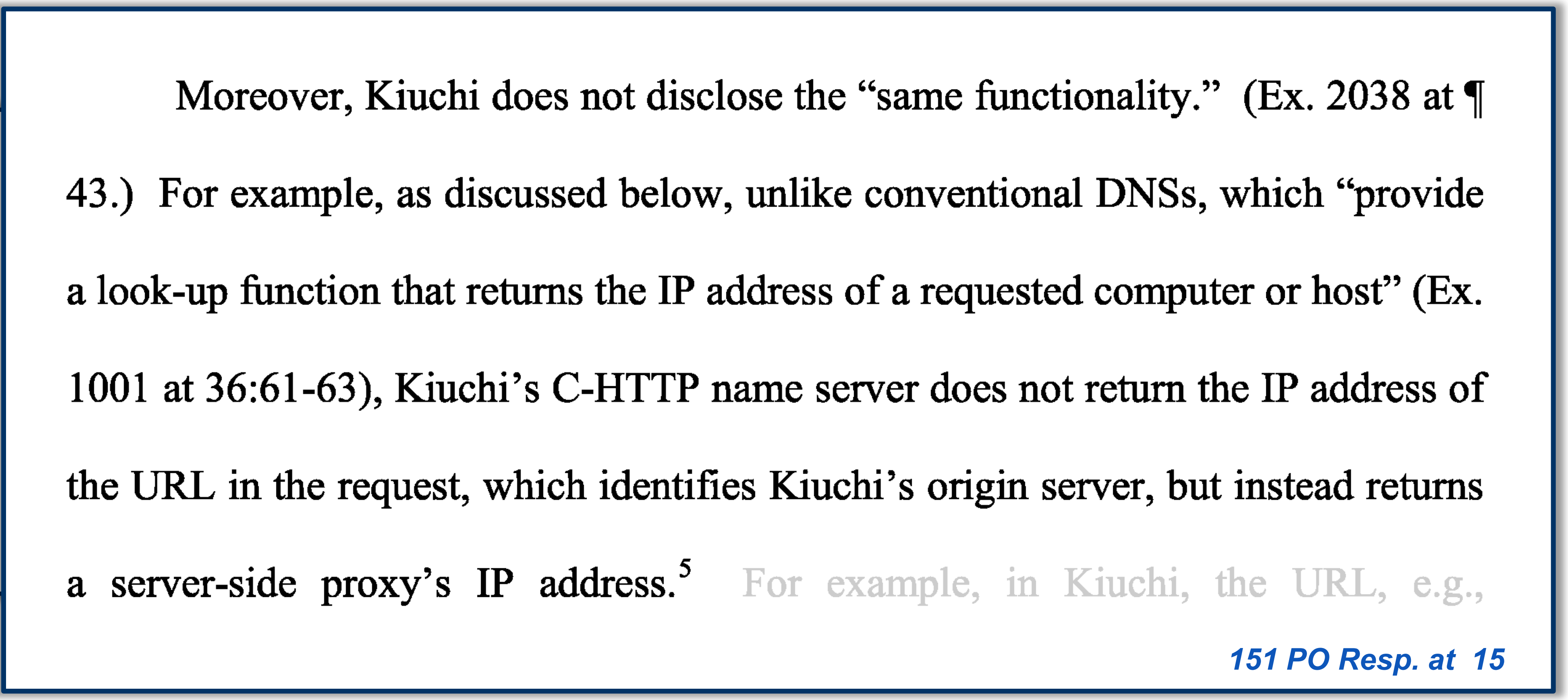
v.

VIRNETX INC.,
Patent Owner

Case IPR2015-01047[1]
Patent 7,490,151

Patent Owner's Response

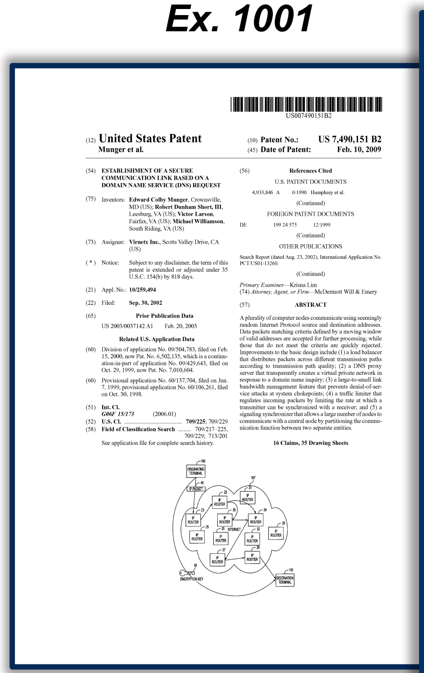
[1] Apple Inc. and Black Swamp IP, LLC, who filed petitions in IPR2016-00063 and IPR2016-00167, respectively, have been joined as a Petitioner in the instant proceeding.



Moreover, Kiuchi does not disclose the "same functionality." (Ex. 2038 at ¶ 43.) For example, as discussed below, unlike conventional DNSs, which "provide a look-up function that returns the IP address of a requested computer or host" (Ex. 1001 at 36:61-63), Kiuchi's C-HTTP name server does not return the IP address of the URL in the request, which identifies Kiuchi's origin server, but instead returns a server-side proxy's IP address.[5] For example, in Kiuchi, the URL, e.g.,

151 PO Resp. at 15

151 Patent Ex. 1001



US007490151B2

(12) **United States Patent**
Munger et al.

(10) **Patent No.: US 7,490,151 B2**
(45) **Date of Patent: Feb. 10, 2009**

(54) **ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST**

(75) Inventors: **Edward Colby Munger**, Crownsville, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/259,494**

(22) Filed: **Sep. 30, 2002**

(65) **Prior Publication Data**

US 2003/0037142 A1 Feb. 20, 2003

Related U.S. Application Data

(60) Division 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.** **709/225**; 709/229

(58) **Field of Classification Search** 709/217–225, 709/229; 713/201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

(Continued)

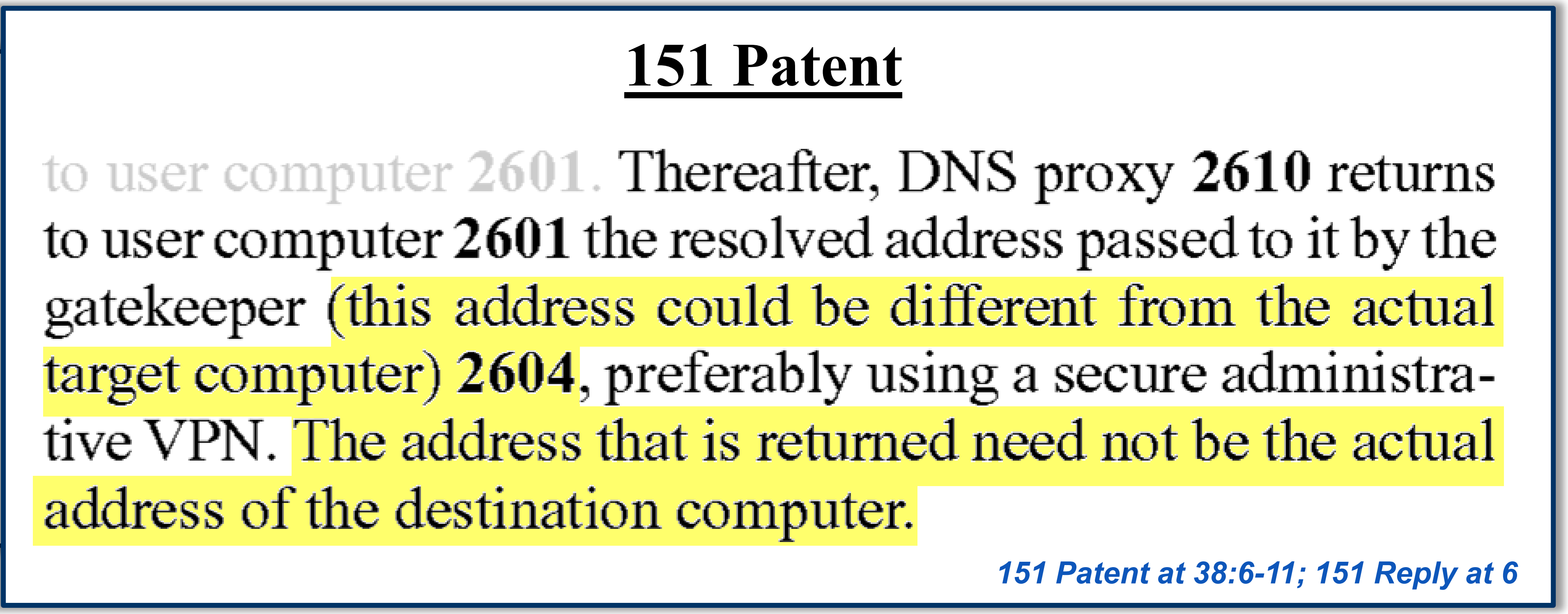
Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emery

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design 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.

16 Claims, 35 Drawing Sheets

100
ORIGINATING TERMINAL
40
IP PACKET
107
22
IP ROUTER
31
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
29
IP ROUTER
25
INTERNET
IP ROUTER
32
IP ROUTER
28
IP ROUTER
27
IP ROUTER
26
IP ROUTER
48
ENCRYPTION KEY
110
DESTINATION TERMINAL



151 Patent

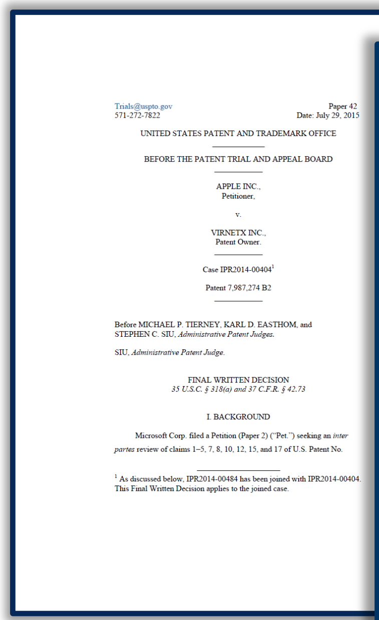
to user computer 2601. Thereafter, DNS proxy **2610** returns to user computer **2601** the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) **2604**, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

151 Patent at 38:6-11; 151 Reply at 6

IPR2014-00404: Kiuchi’s Server-Side Proxy Is the “Host”

Apple Inc. v. VirnetX, Final Written Decision (Paper 42)

IPR2014-00404
Paper 42



Trials@uspto.gov
571-272-7822

Paper 42
Date: July 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00404[1]

Patent 7,987,274 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

SIU, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

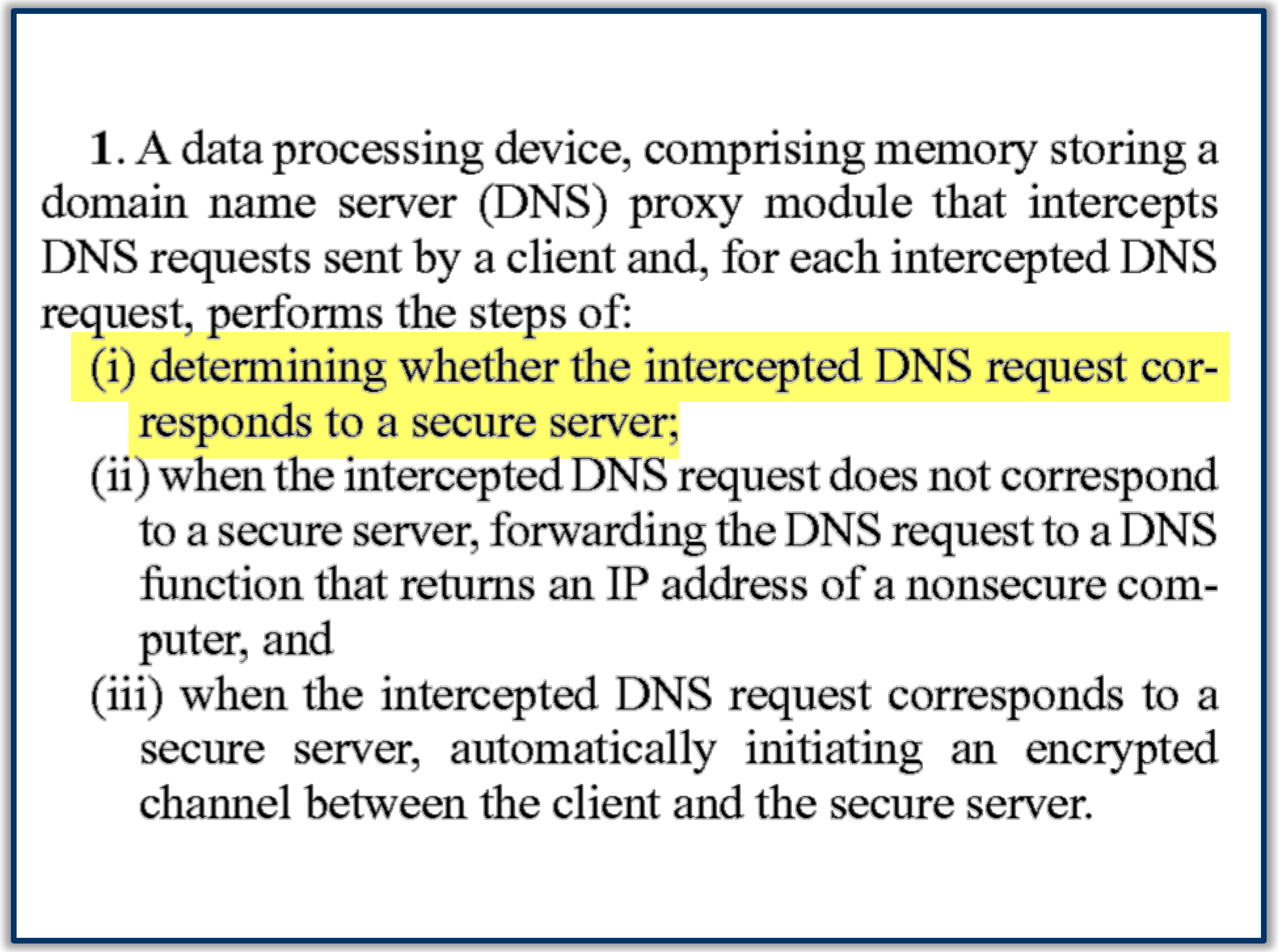
Microsoft Corp. filed a Petition (Paper 2) (“Pet.”) seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 15, and 17 of U.S. Patent No.

[1] As discussed below, IPR2014-00484 has been joined with IPR2014-00404. This Final Written Decision applies to the joined case.

Patent Owner argues that Kiuchi discloses that the client-side proxy sends a request for a network address for the “origin server” but not for the server-side proxy. However, Kiuchi discloses that in response to the request to communicate with “the host,” the name server examines “the requested *server-side proxy*” and returns “the IP address . . . of the *server-side proxy*.” Ex. 1004, 65 (emphasis added). Thus, contrary to Patent Owner’s contention, “the host” of Kiuchi corresponds to the “server-side proxy” (or second network device, as recited in claim 1).

Final Written Decision (Paper 42) at 11-12; 135 Reply at 7; 151 Reply at 6

151 Patent

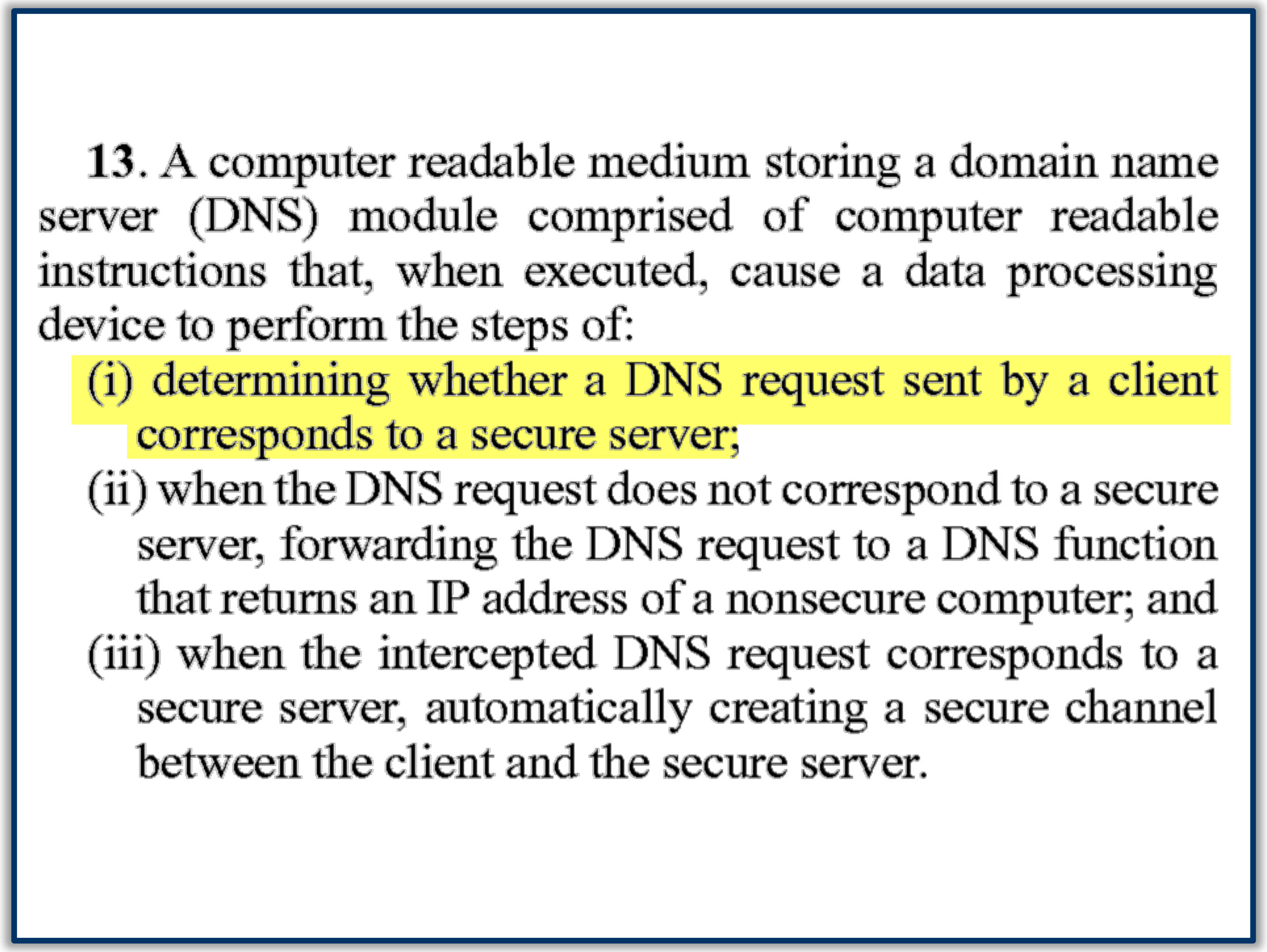


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.



13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

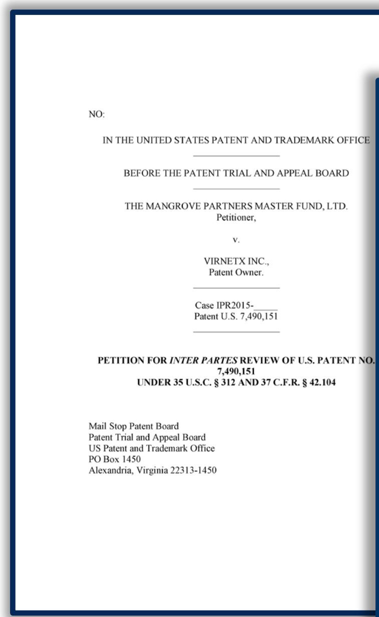
(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

Kiuchi

"*determining*"

Petition
Paper 5



NO:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD.
Petitioner,

v.

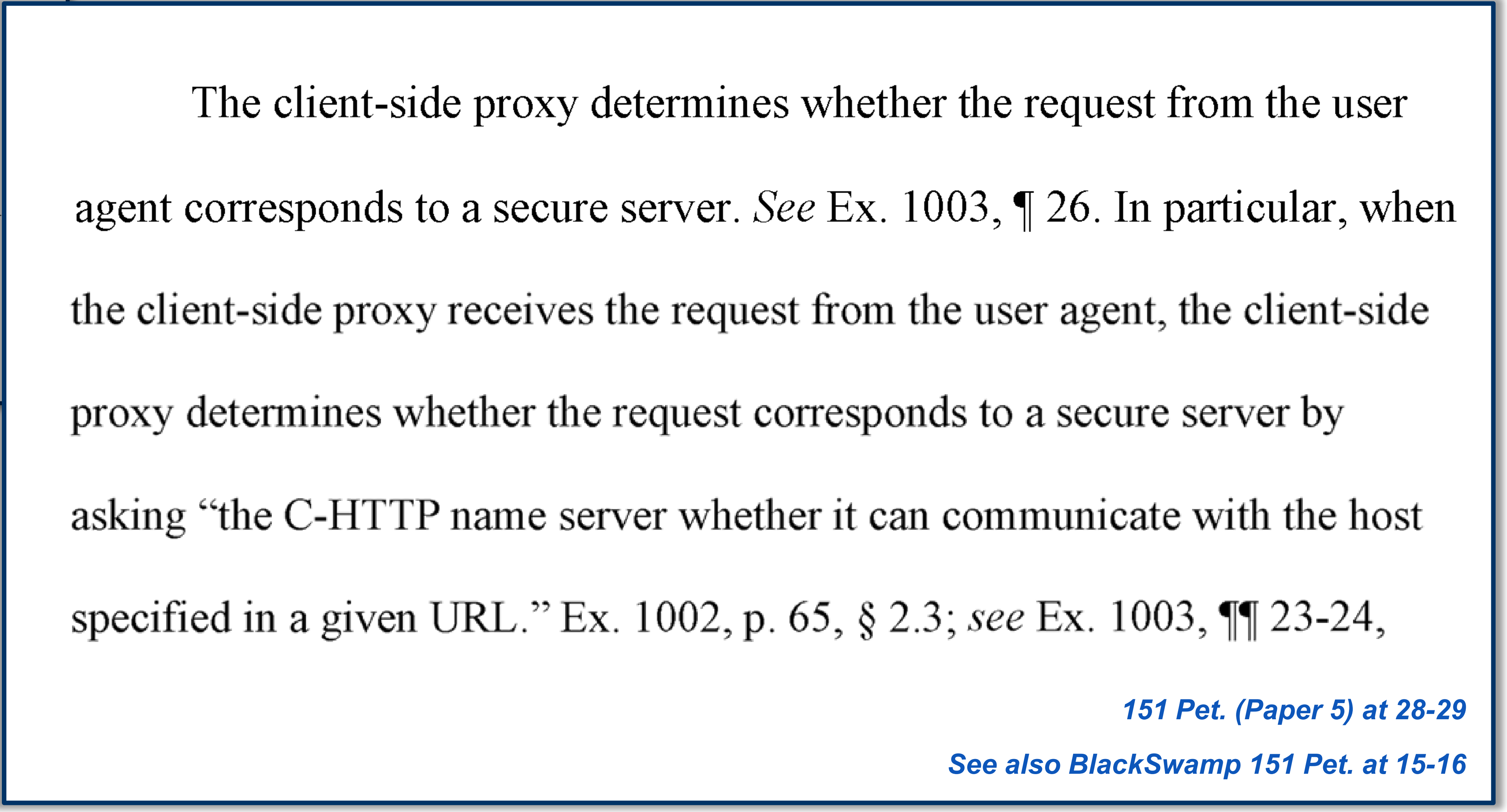
VIRNETX INC.,
Patent Owner.

Case IPR2015-_____
Patent U.S. 7,490,151

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,490,151
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

Mail Stop Patent Board
Patent Trial and Appeal Board
US Patent and Trademark Office
PO Box 1450
Alexandria, Virginia 22313-1450

Petition



The client-side proxy determines whether the request from the user agent corresponds to a secure server. *See* Ex. 1003, ¶ 26. In particular, when the client-side proxy receives the request from the user agent, the client-side proxy determines whether the request corresponds to a secure server by asking "the C-HTTP name server whether it can communicate with the host specified in a given URL." Ex. 1002, p. 65, § 2.3; *see* Ex. 1003, ¶¶ 23-24,

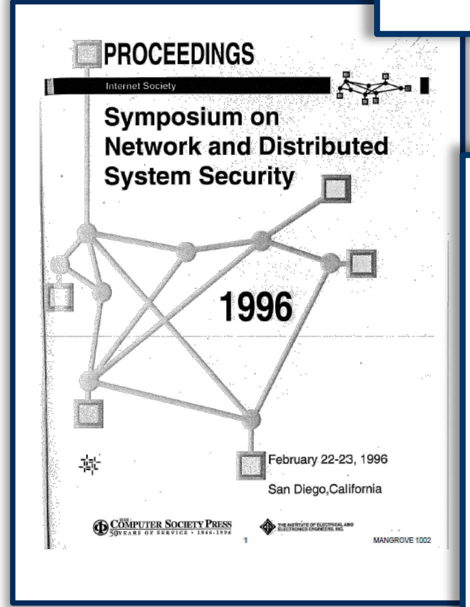
151 Pet. (Paper 5) at 28-29

See also BlackSwamp 151 Pet. at 15-16

Kiuchi

"determining"

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

Symposium on
Network and Distributed
System Security

1996

February 22-23, 1996

San Diego,California

IEEE COMPUTER SOCIETY PRESS
50 YEARS OF SERVICE • 1946-1996

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

1

MANGROVE 1002

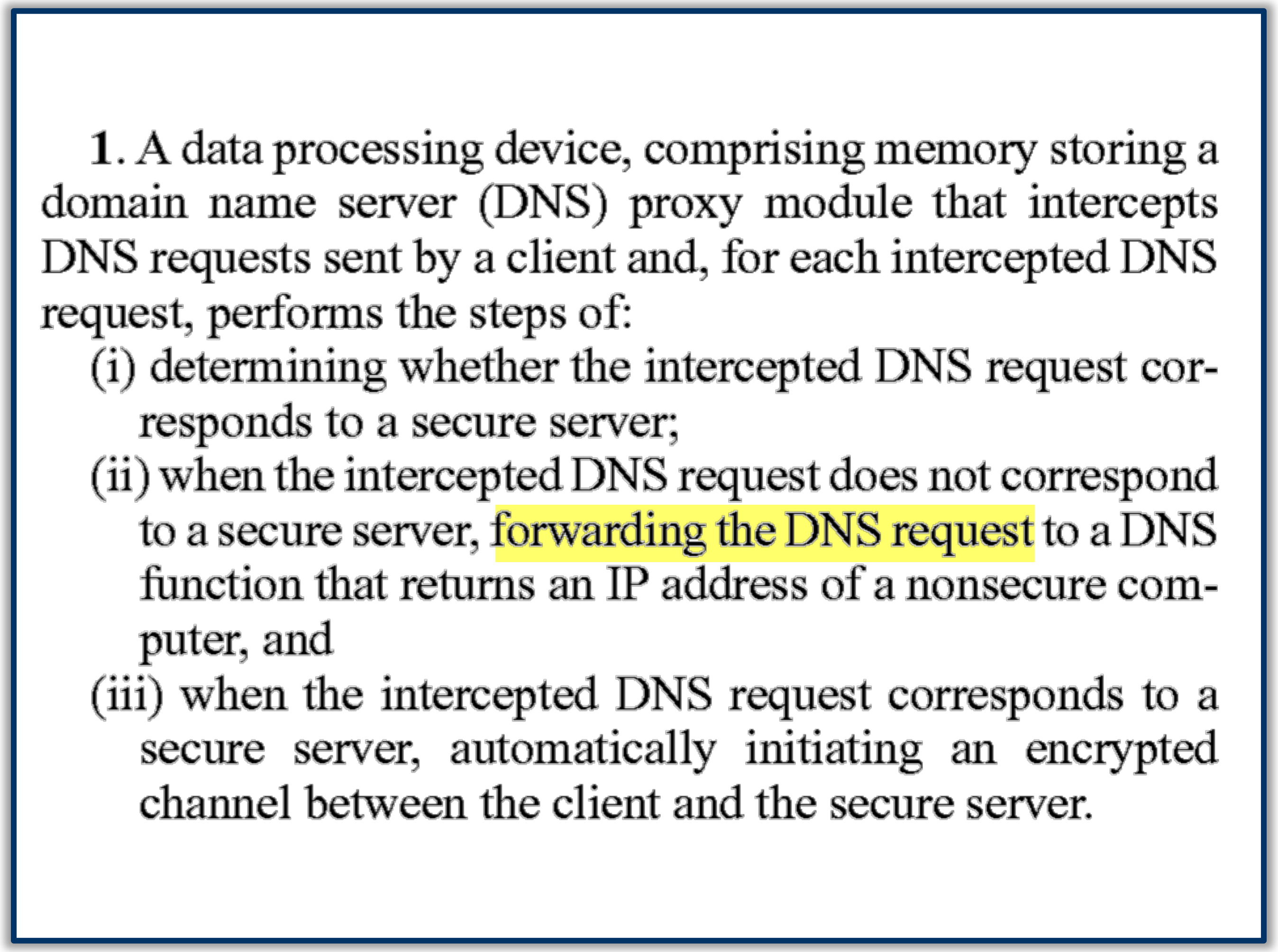
C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

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. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.

Kiuchi at 65; 151 Pet. at 28-29

151 Patent

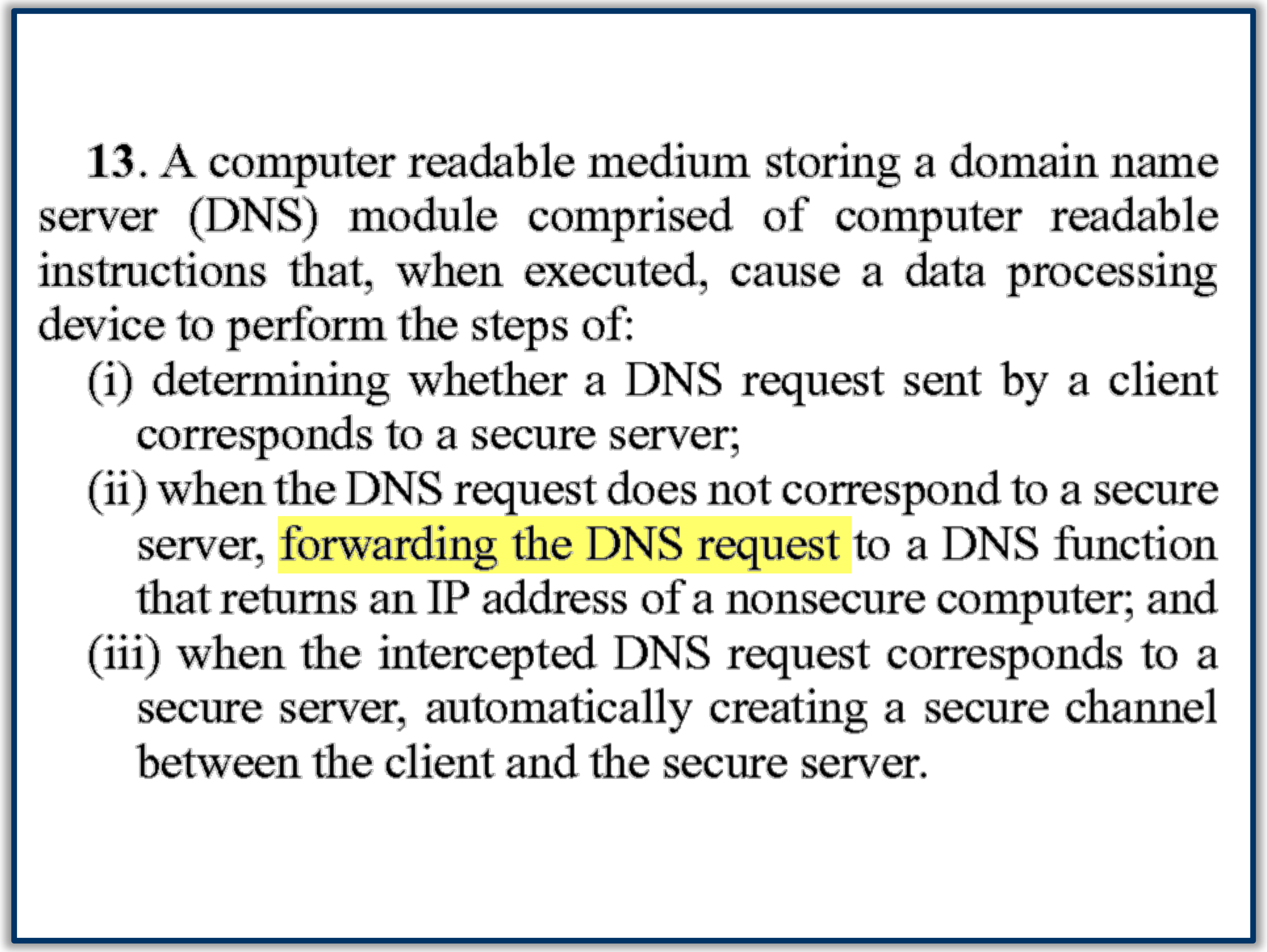


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.



13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

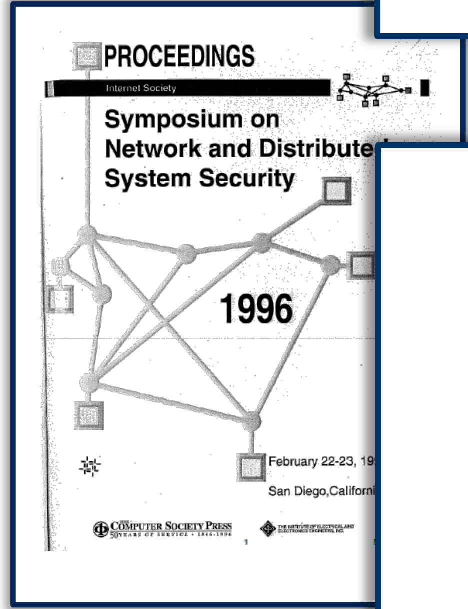
(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

Kiuchi

"forwarding the DNS request"

Kiuchi* *Ex. 1002



PROCEEDINGS

Internet Society

Symposium on Network and Distribute

System Security

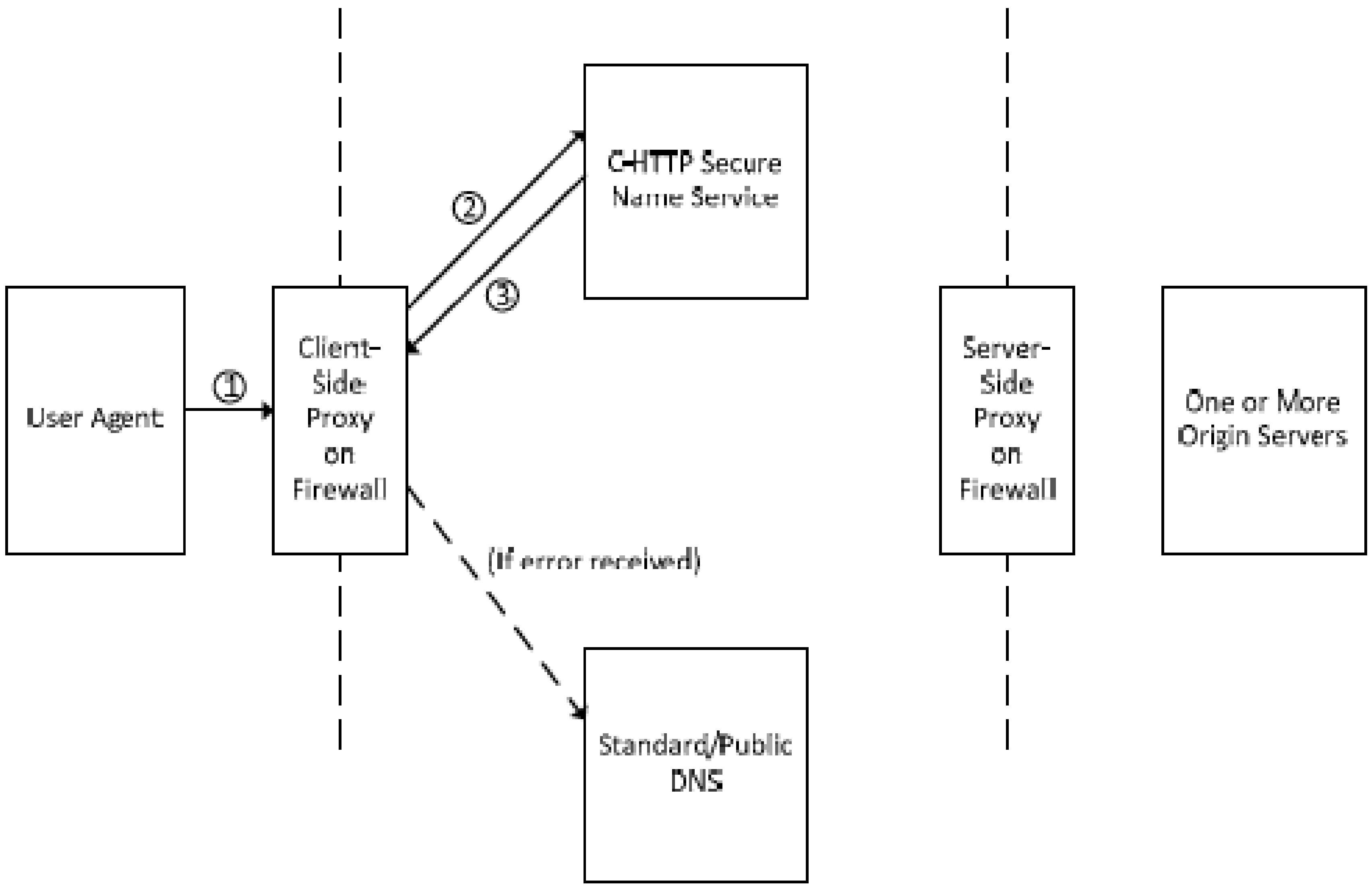
1996

February 22-23, 19

San Diego,Californi

Computer Society Press

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

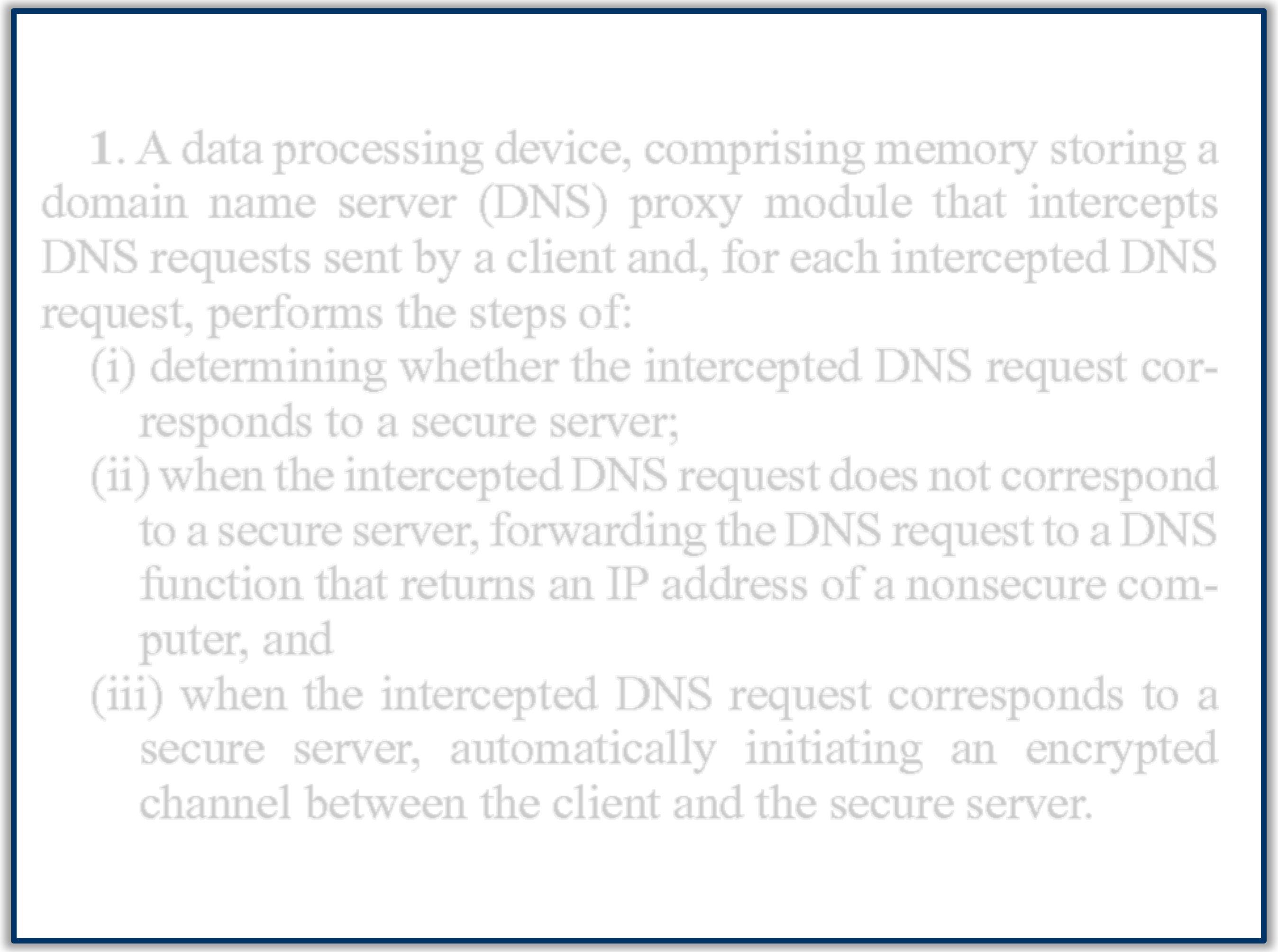


User Agent
①
Client-Side Proxy on Firewall
②
③
C-HTTP Secure Name Service
(If error received)
Standard/Public DNS
Server-Side Proxy on Firewall
One or More Origin Servers

Diagram 3

151 Pet. (Paper 5) at 20

151 Patent

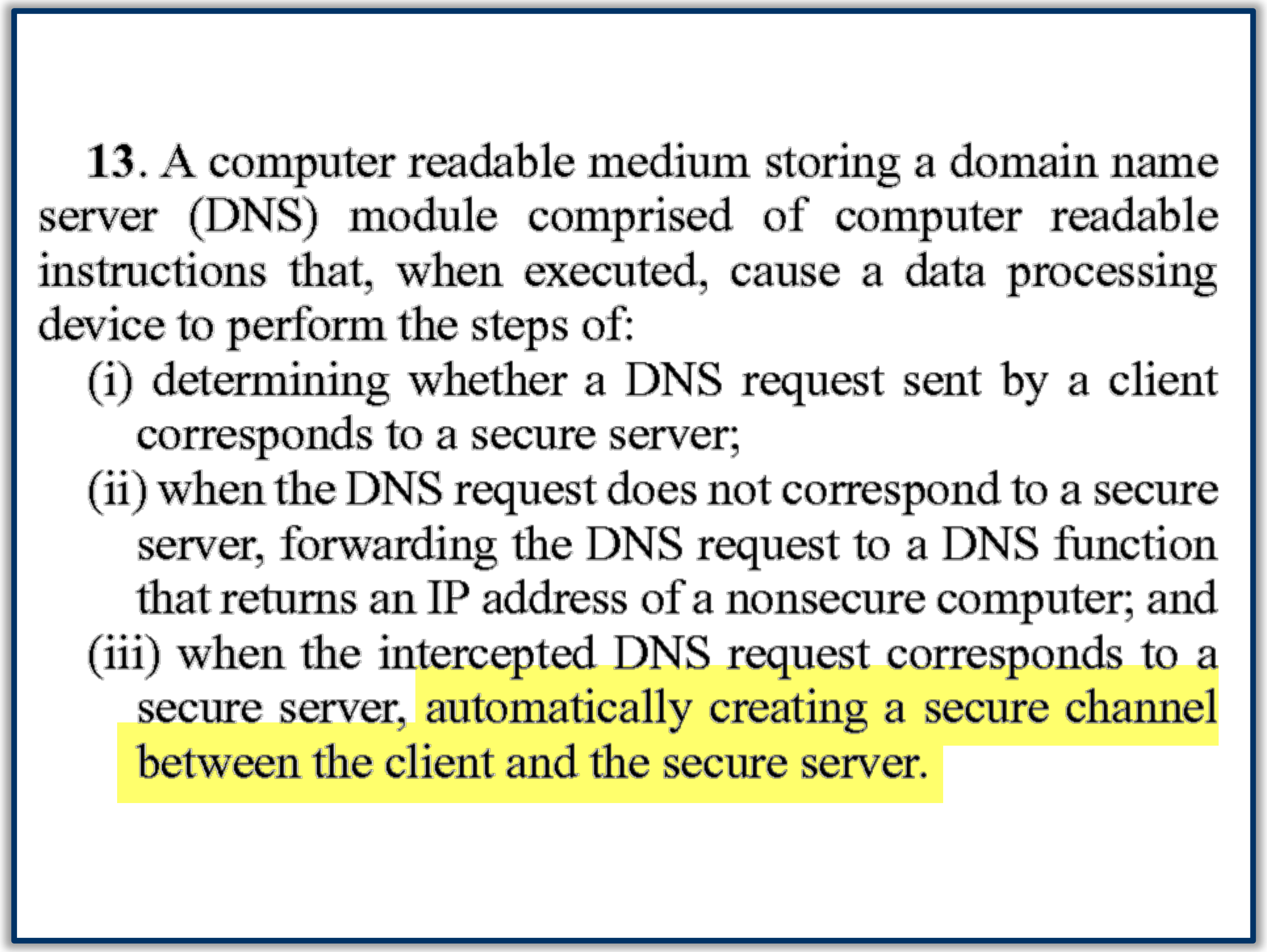


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.



13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) determining whether a DNS request sent by a client corresponds to a secure server;

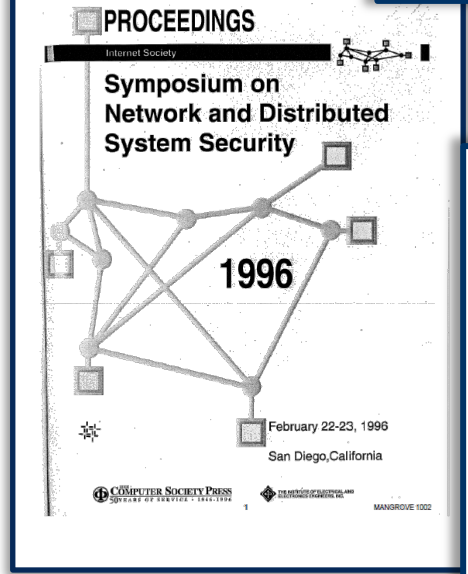
(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

Kiuchi

“automatically creating a secure channel”

Kiuchi
Ex. 1002



PROCEEDINGS

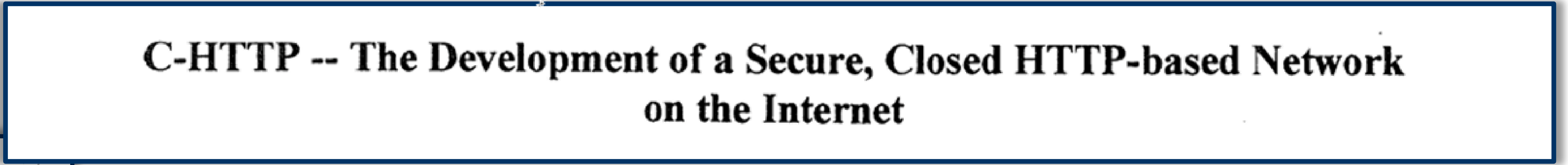
Internet Society

Symposium on
Network and Distributed
System Security

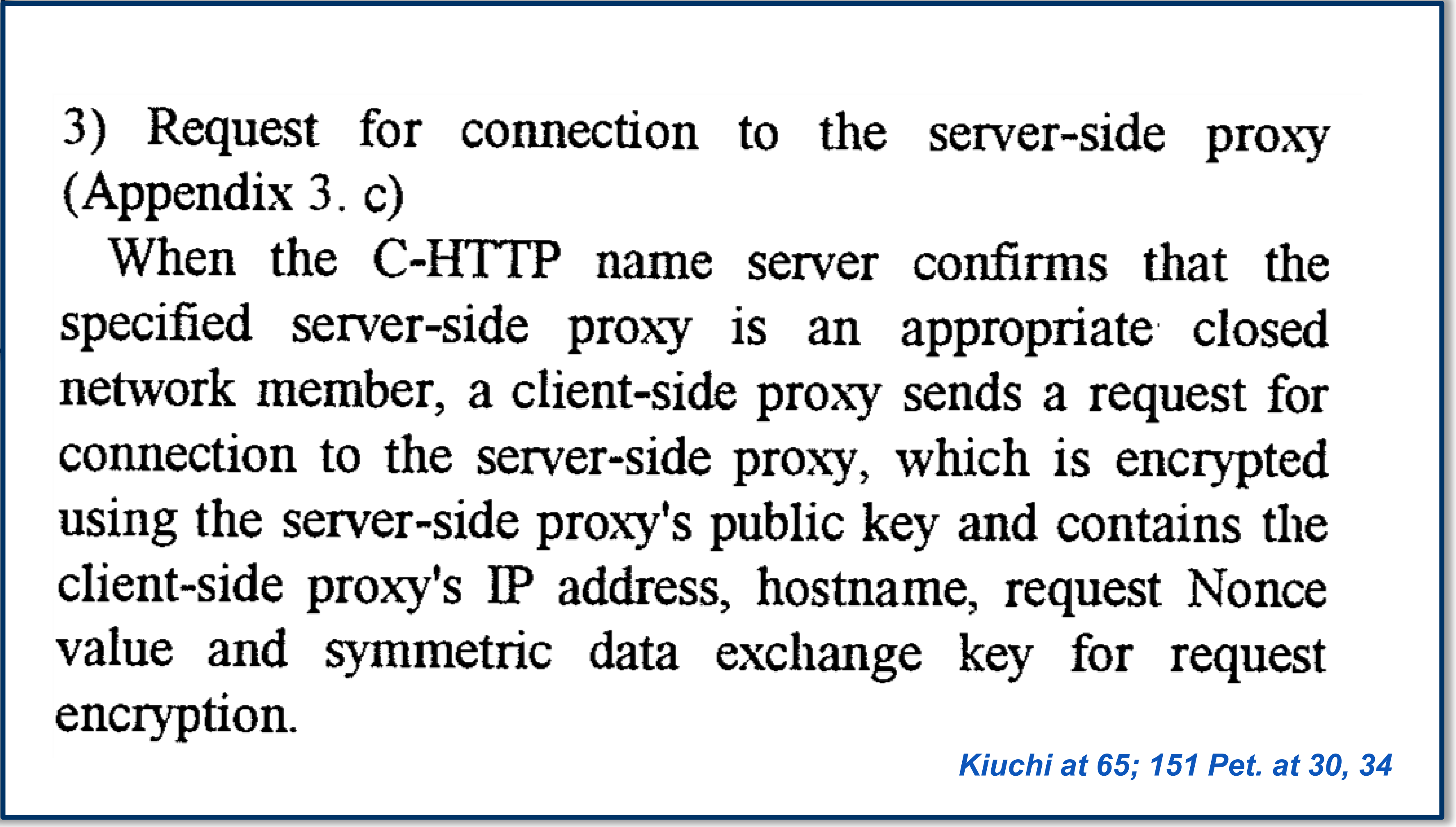
1996

February 22-23, 1996
San Diego,California

MANGROVE 1002



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



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

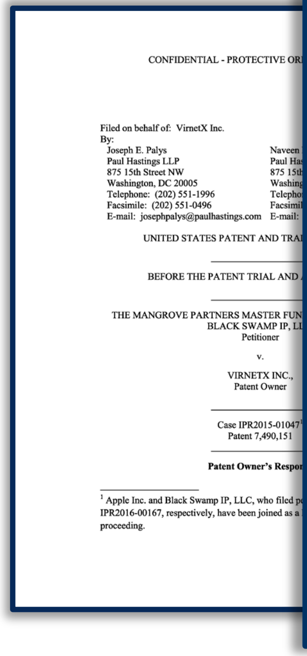
When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client-side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy's public key and contains the client-side proxy's IP address,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

Kiuchi at 65; 151 Pet. at 30, 34

Patent Owner Assertion

Does not address "secure channel" with respect to user agent and origin server

Respon
Paper 4



CONFIDENTIAL - PROTECTIVE OR

Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings.com

Naveen
Paul Ha
875 15th
Washing
Telepho
Facsimil
E-mail:

UNITED STATES PATENT AND TRA

BEFORE THE PATENT TRIAL AND

THE MANGROVE PARTNERS MASTER FUN
BLACK SWAMP IP, LL
Petitioner

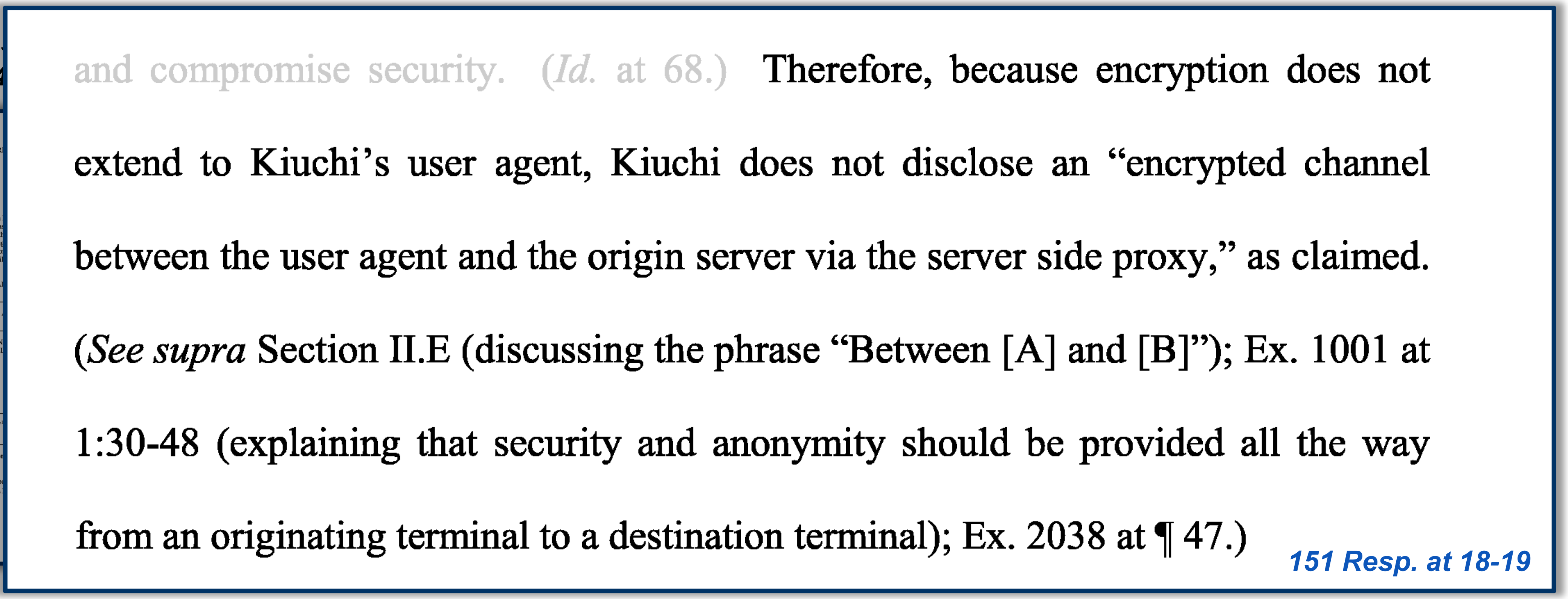
v.

VIRNETX INC.,
Patent Owner

Case IPR2015-01047[1]
Patent 7,490,151

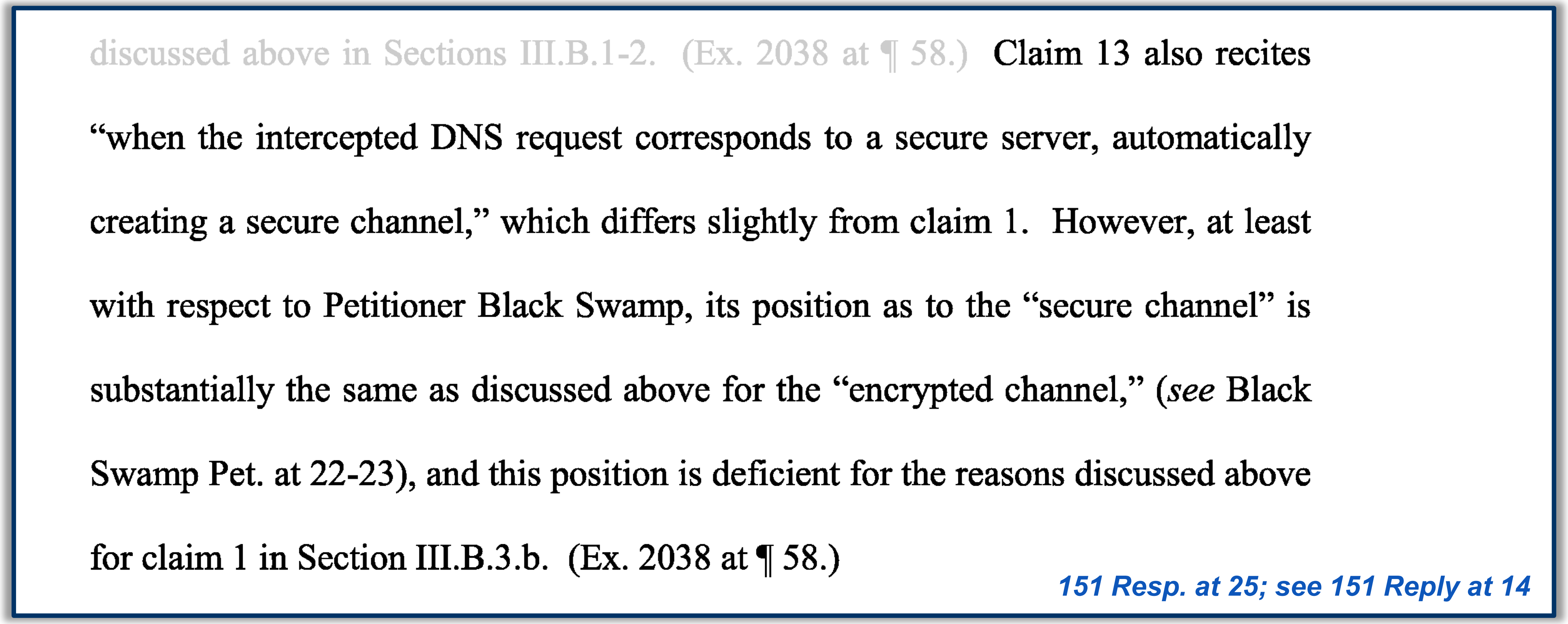
Patent Owner's Respo

[1] Apple Inc. and Black Swamp IP, LLC, who filed p
IPR2016-00167, respectively, have been joined as a
proceeding.



and compromise security. (*Id.* at 68.) Therefore, because encryption does not extend to Kiuchi's user agent, Kiuchi does not disclose an "encrypted channel between the user agent and the origin server via the server side proxy," as claimed. (*See supra* Section II.E (discussing the phrase "Between [A] and [B]"); Ex. 1001 at 1:30-48 (explaining that security and anonymity should be provided all the way from an originating terminal to a destination terminal); Ex. 2038 at ¶ 47.)

151 Resp. at 18-19

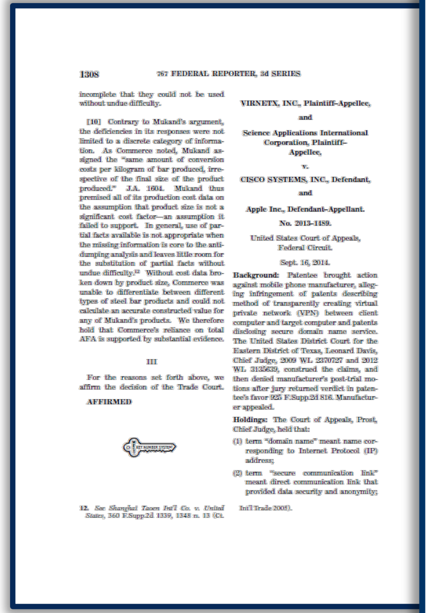


discussed above in Sections III.B.1-2. (Ex. 2038 at ¶ 58.) Claim 13 also recites "when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel," which differs slightly from claim 1. However, at least with respect to Petitioner Black Swamp, its position as to the "secure channel" is substantially the same as discussed above for the "encrypted channel," (*see* Black Swamp Pet. at 22-23), and this position is deficient for the reasons discussed above for claim 1 in Section III.B.3.b. (Ex. 2038 at ¶ 58.)

151 Resp. at 25; see 151 Reply at 14

VirnetX v. Cisco, 767 F.3d 1308 (Fed. Cir. 2014)

VirnetX v. Cisco
(Fed. Cir. 2014)



1308 767 FEDERAL REPORTER, 3d SERIES

incomplete that they could not be used without undue difficulty.

[10] Contrary to Mukand's argument, the deficiencies in its responses were not limited to a discrete category of information. As Commerce noted, Mukand assigned the "same amount of conversion costs per kilogram of bar produced, irrespective of the final size of the product produced." J.A. 1604. Mukand thus premised all of its production cost data on the assumption that product size is not a significant cost factor—an assumption it failed to support. In general, use of partial facts available is not appropriate when the missing information is core to the antidumping analysis and leaves little room for the substitution of partial facts without undue difficulty.[12] Without cost data broken down by product size, Commerce was unable to differentiate between different types of steel bar products and could not calculate an accurate constructed value for any of Mukand's products. We therefore hold that Commerce's reliance on total AFA is supported by substantial evidence.

III

For the reasons set forth above, we affirm the decision of the Trade Court.

AFFIRMED

VIRNETX, INC., Plaintiff–Appellee,

and

Science Applications International Corporation, Plaintiff–Appellee,

v.

CISCO SYSTEMS, INC., Defendant,

and

Apple Inc., Defendant–Appellant.

No. 2013–1489.

United States Court of Appeals, Federal Circuit.

Sept. 16, 2014.

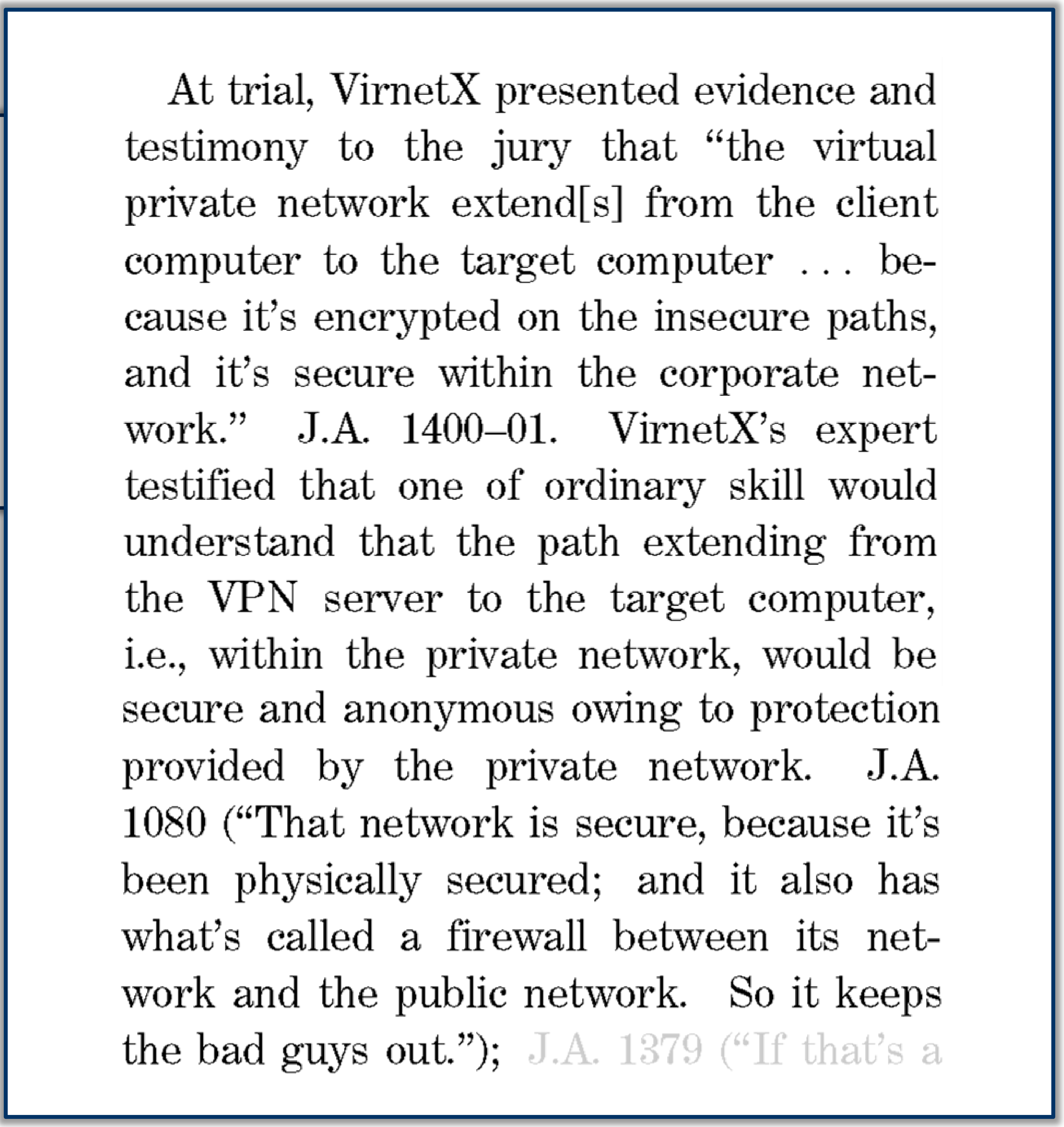
Background: Patentee brought action against mobile phone manufacturer, alleging infringement of patents describing method of transparently creating virtual private network (VPN) between client computer and target computer and patents disclosing secure domain name service. The United States District Court for the Eastern District of Texas, Leonard Davis, Chief Judge, 2009 WL 2370727 and 2012 WL 3135639, construed the claims, and then denied manufacturer's post-trial motions after jury returned verdict in patentee's favor 925 F.Supp.2d 816. Manufacturer appealed.

Holdings: The Court of Appeals, Prost, Chief Judge, held that:

(1) term "domain name" meant name corresponding to Internet Protocol (IP) address;

(2) term "secure communication link" meant direct communication link that provided data security and anonymity;

[12] *See Shanghai Taoen Int'l Co. v. United States*, 360 F.Supp.2d 1339, 1348 n. 13 (Ct. Int'l Trade 2005).

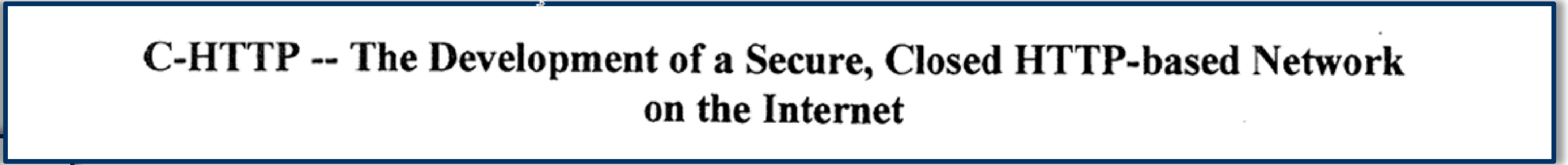


At trial, VirnetX presented evidence and testimony to the jury that "the virtual private network extend[s] from the client computer to the target computer . . . because it's encrypted on the insecure paths, and it's secure within the corporate network." J.A. 1400–01. VirnetX's expert testified that one of ordinary skill would understand that the path extending from the VPN server to the target computer, i.e., within the private network, would be secure and anonymous owing to protection provided by the private network. J.A. 1080 ("That network is secure, because it's been physically secured; and it also has what's called a firewall between its network and the public network. So it keeps the bad guys out."); J.A. 1379 ("If that's a

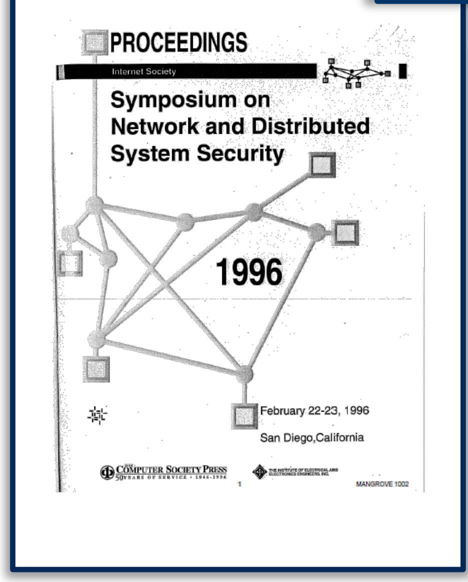
VirnetX, 767 F.3d at 1321
135 Reply at 12
151 Reply at 14

Kiuchi

Kiuchi
Ex. 1002



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



PROCEEDINGS

Internet Society

Symposium on
Network and Distributed
System Security

1996

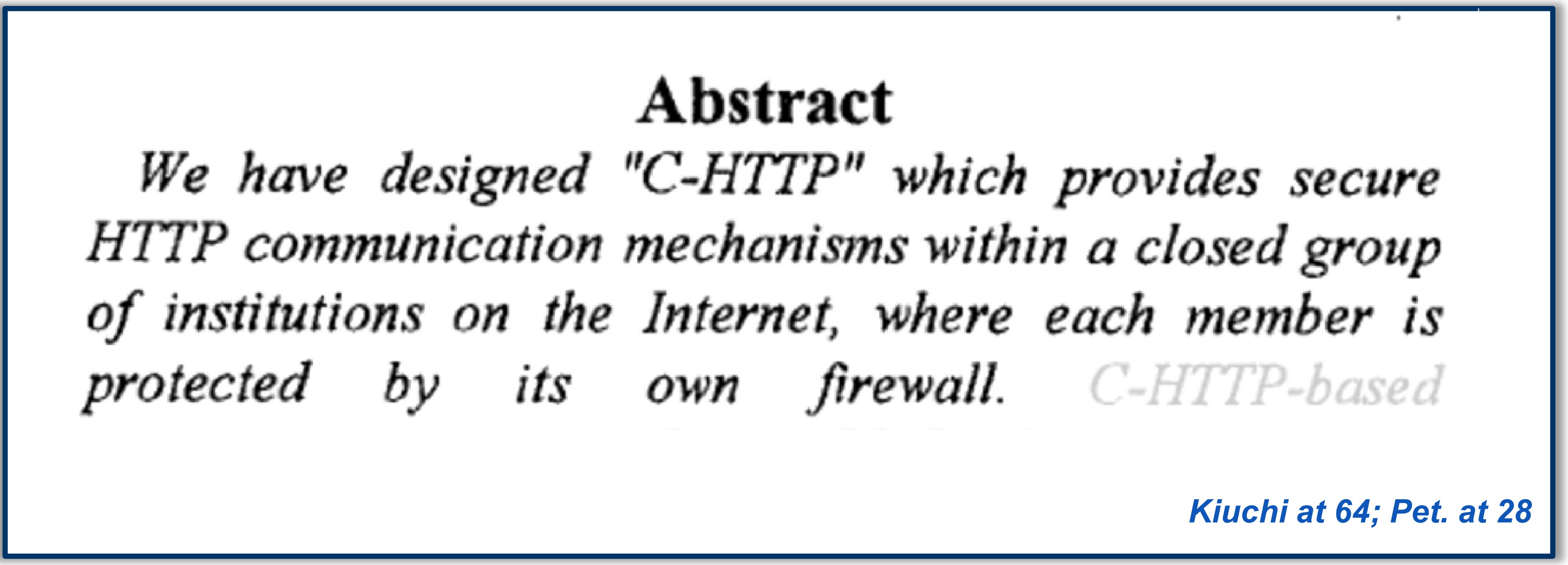
February 22-23, 1996
San Diego,California

COMPUTER SOCIETY PRESS
50 YEARS OF SERVICE • 1946-1996

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

1

MANGROVE 1002

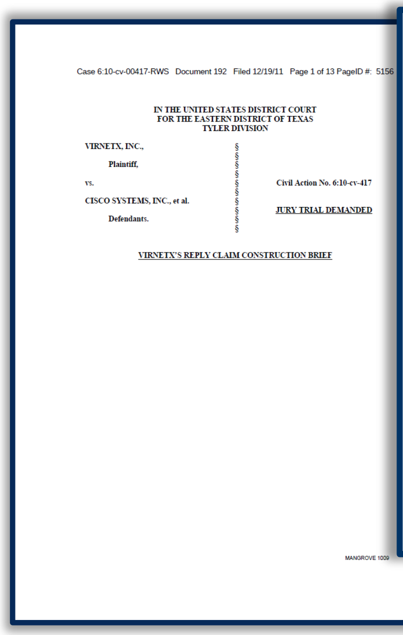


Abstract

We have designed "C-HTTP" which provides secure HTTP communication mechanisms within a closed group of institutions on the Internet, where each member is protected by its own firewall. C-HTTP-based

Kiuchi at 64; Pet. at 28

VirnetX CC Br.
Ex. 1009



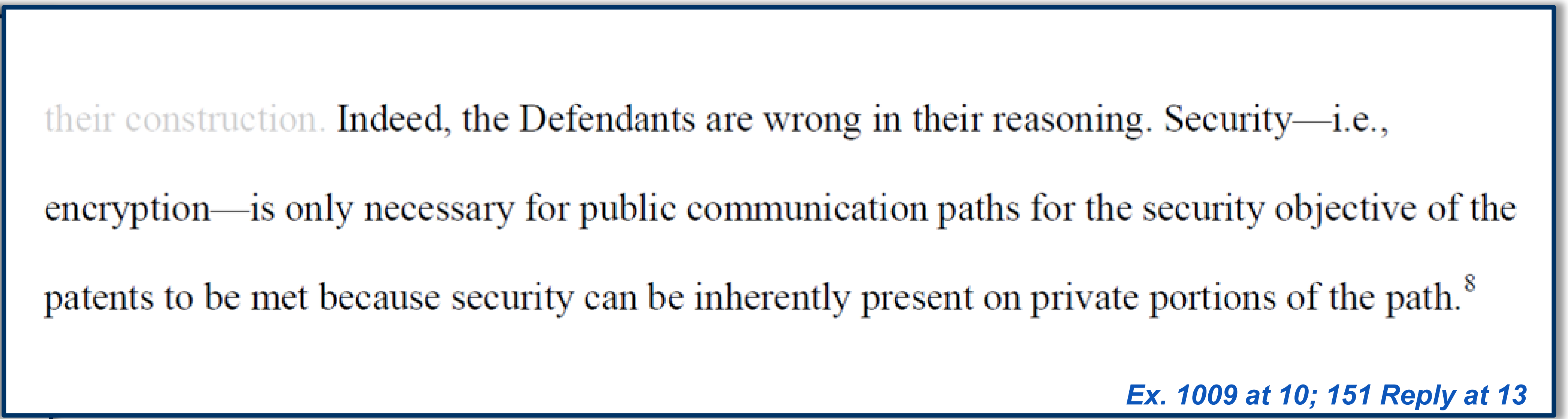
Case 6:10-cv-00417-RWS Document 192 Filed 12/19/11 Page 1 of 13 PageID #: 5156

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX, INC.,	§	
Plaintiff,	§	
vs.	§	Civil Action No. 6:10-cv-417
CISCO SYSTEMS, INC., et al.	§	JURY TRIAL DEMANDED
Defendants.	§	

VIRNETX'S REPLY CLAIM CONSTRUCTION BRIEF

MANGROVE 1009



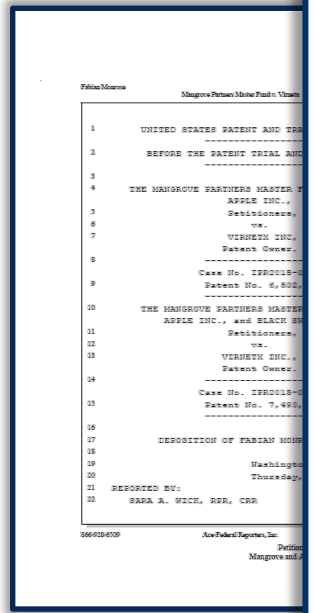
their construction. Indeed, the Defendants are wrong in their reasoning. Security—i.e., encryption—is only necessary for public communication paths for the security objective of the patents to be met because security can be inherently present on private portions of the path.[8]

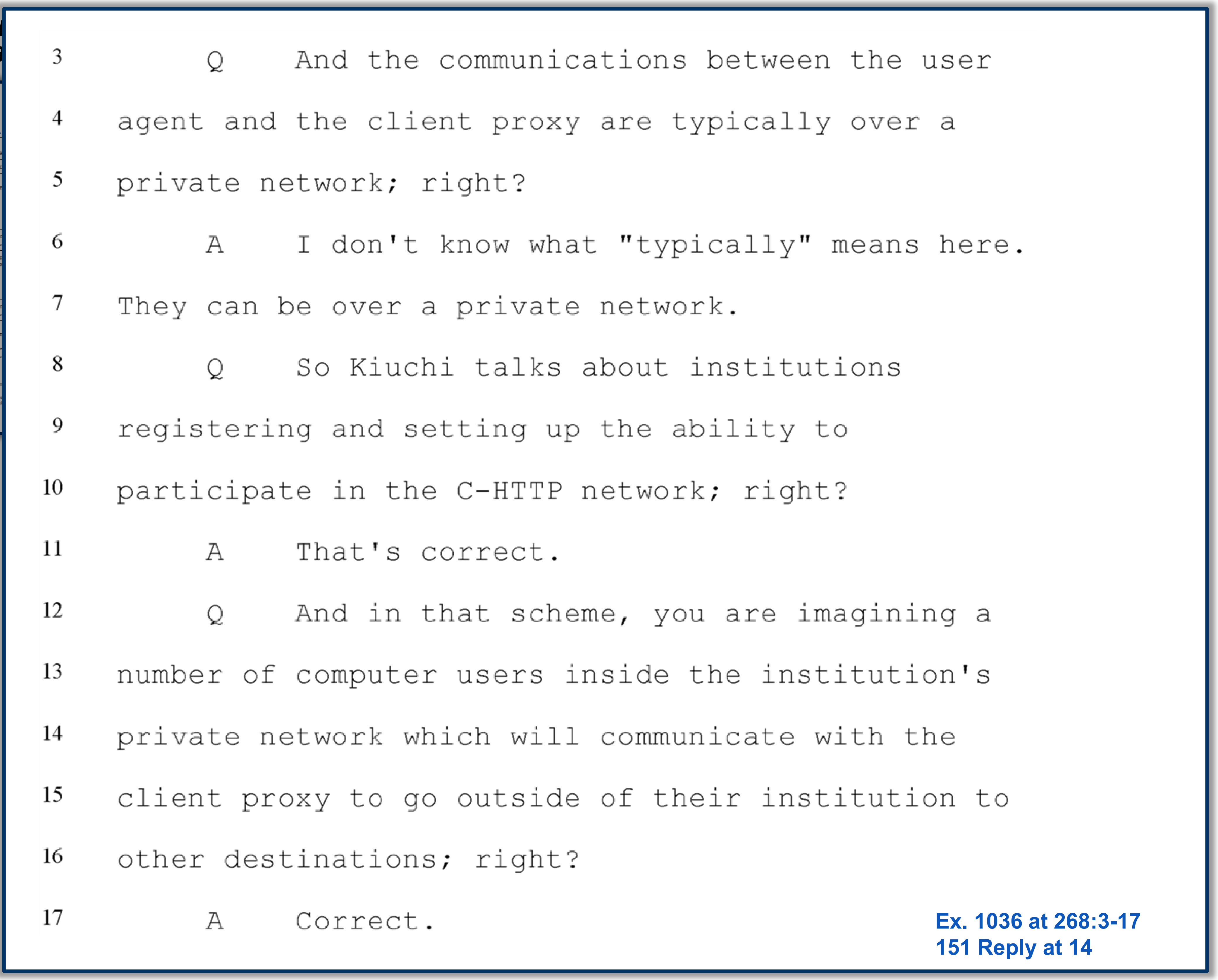
Ex. 1009 at 10; 151 Reply at 13

Kiuchi

Ex. 1036 – Deposition Transcript of Dr. Fabian Monrose (April 28, 2016)

Monrose D
Ex. 103





Q And the communications between the user agent and the client proxy are typically over a private network; right?

A I don't know what "typically" means here. They can be over a private network.

Q So Kiuchi talks about institutions registering and setting up the ability to participate in the C-HTTP network; right?

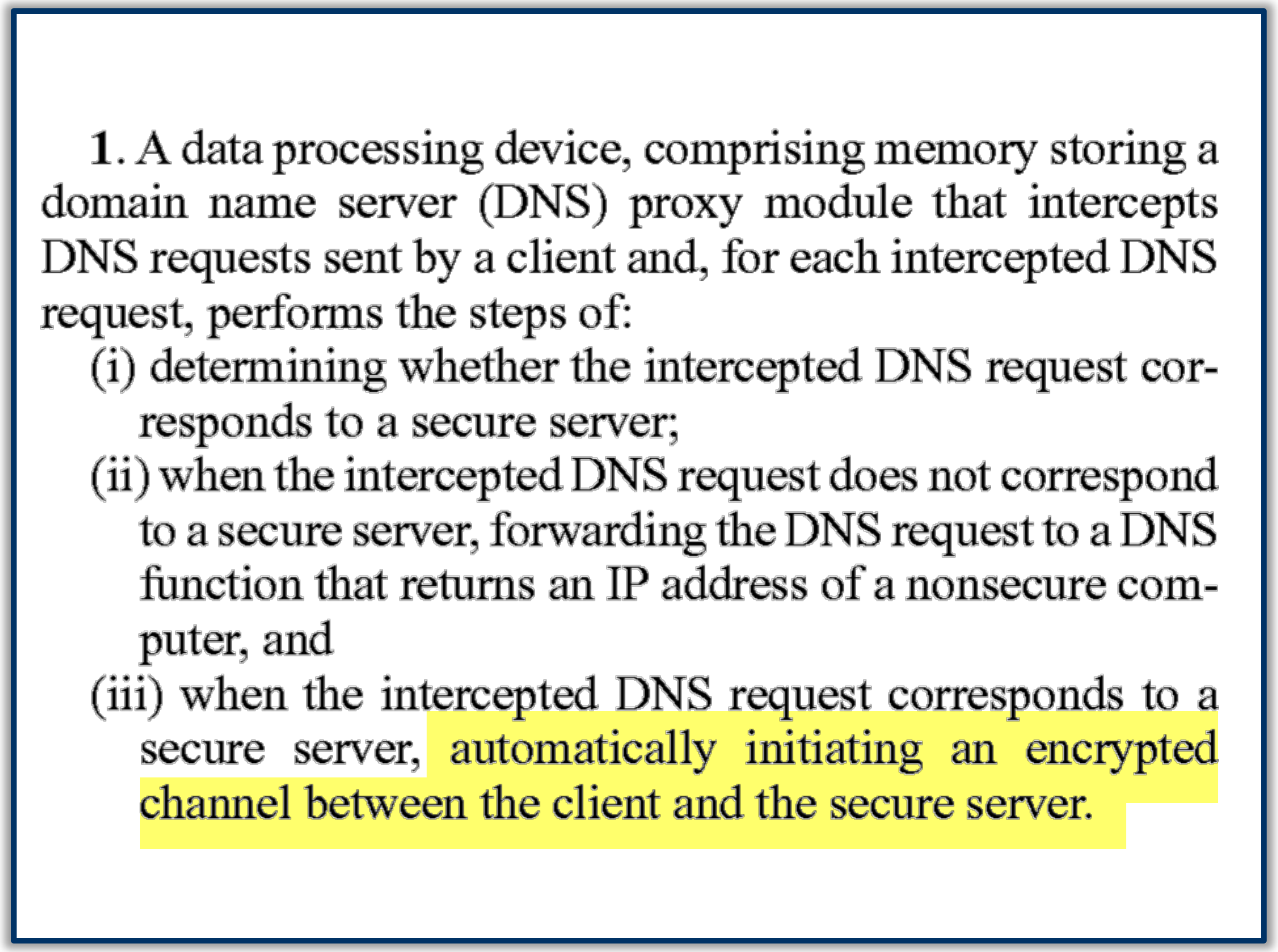
A That's correct.

Q And in that scheme, you are imagining a number of computer users inside the institution's private network which will communicate with the client proxy to go outside of their institution to other destinations; right?

A Correct.

Ex. 1036 at 268:3-17
151 Reply at 14

151 Patent

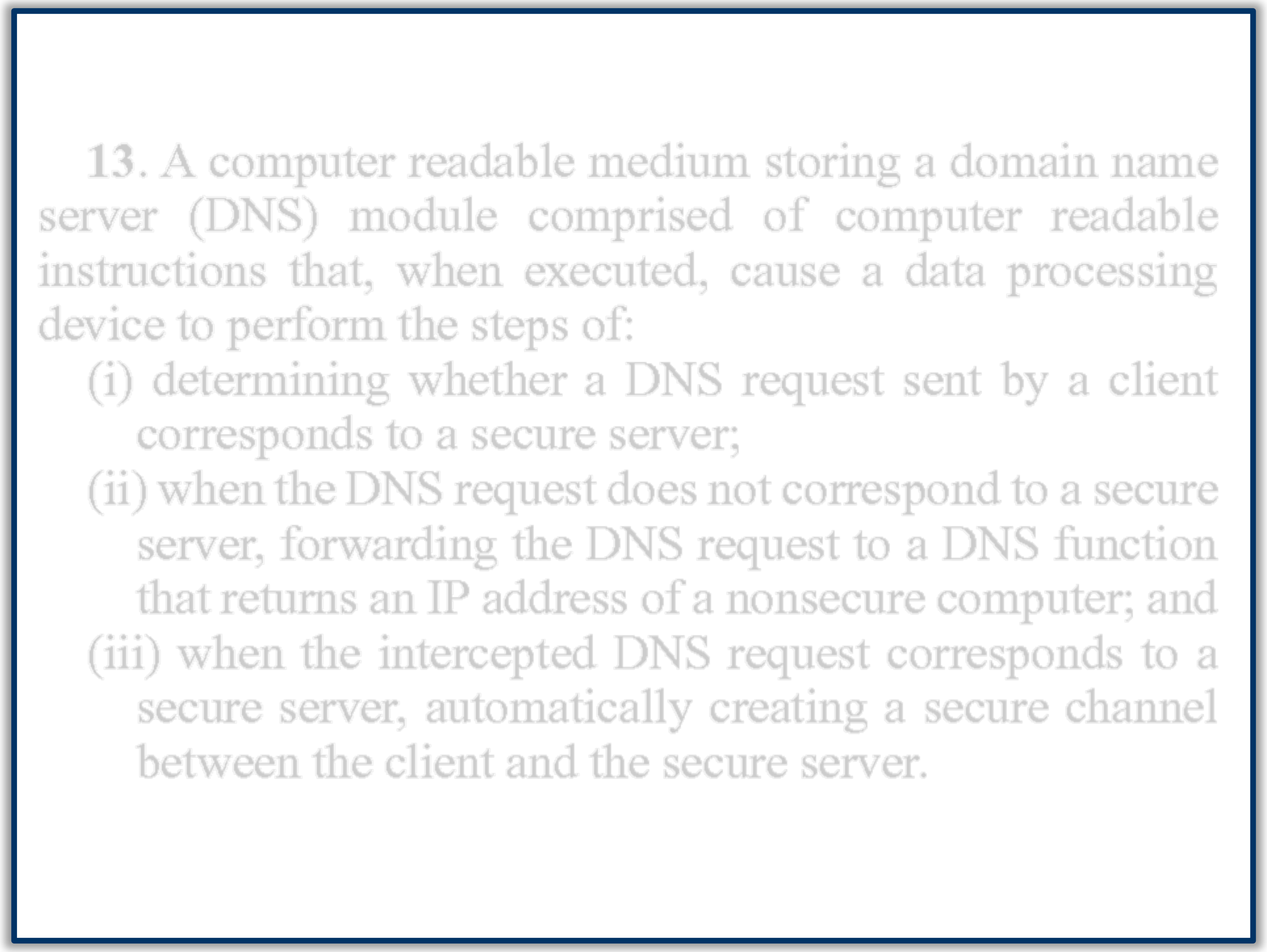


1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:

(i) determining whether the intercepted DNS request corresponds to a secure server;

(ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and

(iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.



13. A computer readable medium storing a domain name server (DNS) module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

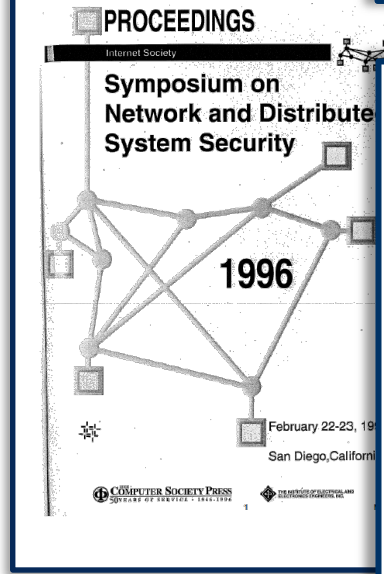
(i) determining whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server.

Kiuchi Works with Other Security Protocols

Kiuchi
Ex. 1002


PROCEEDINGS

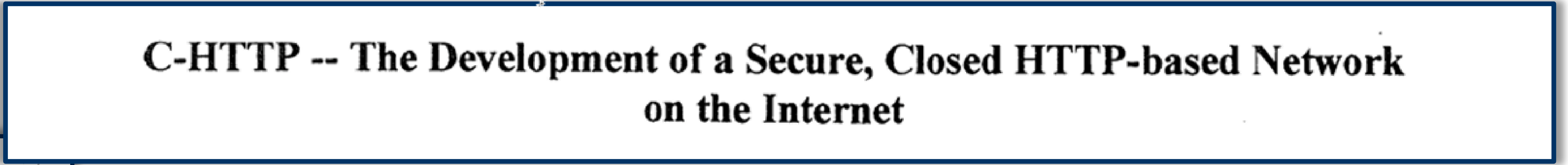
Internet Society

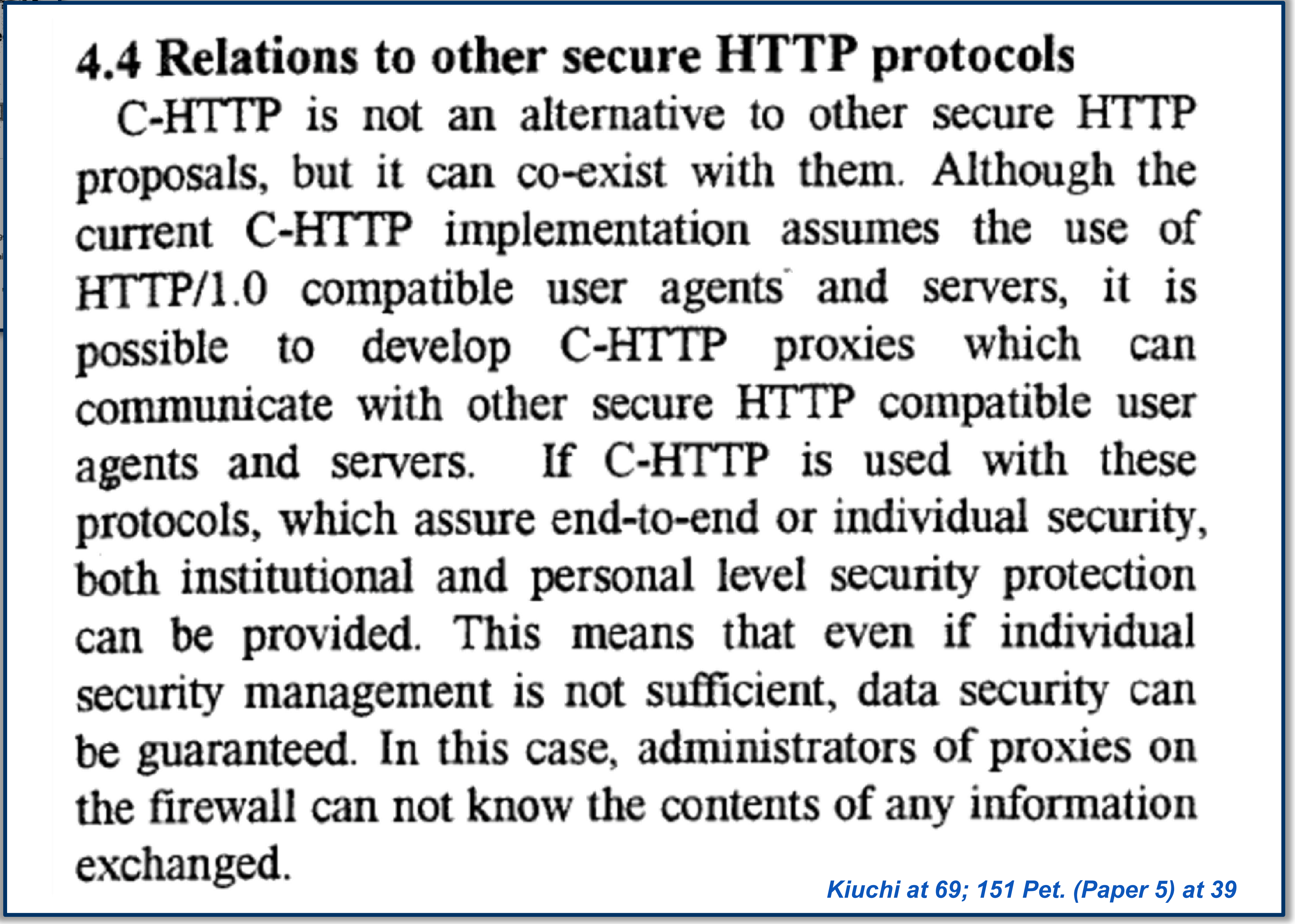
Symposium on
Network and Distribute
System Security

1996

February 22-23, 19

San Diego,Californi


C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

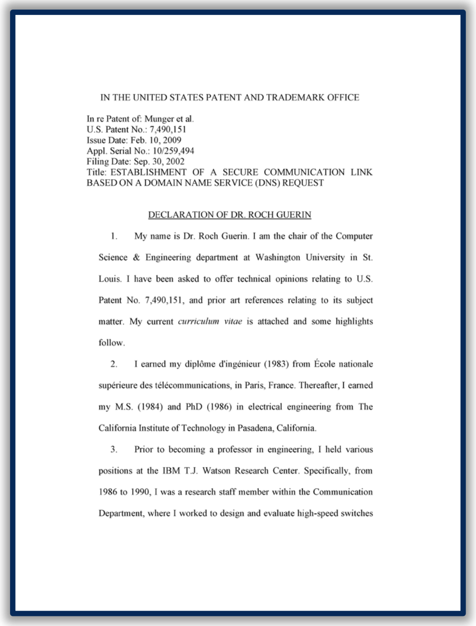

4.4 Relations to other secure HTTP protocols

C-HTTP is not an alternative to other secure HTTP proposals, but it can co-exist with them. Although the current C-HTTP implementation assumes the use of HTTP/1.0 compatible user agents and servers, it is possible to develop C-HTTP proxies which can communicate with other secure HTTP compatible user agents and servers. If C-HTTP is used with these protocols, which assure end-to-end or individual security, both institutional and personal level security protection can be provided. This means that even if individual security management is not sufficient, data security can be guaranteed. In this case, administrators of proxies on the firewall can not know the contents of any information exchanged.

Kiuchi at 69; 151 Pet. (Paper 5) at 39

Dr. Guerin: Rescorla Teaches End-to-End Encryption

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger et al.
U.S. Patent No.: 7,490,151
Issue Date: Feb. 10, 2009
Appl. Serial No.: 10/259,494
Filing Date: Sep. 30, 2002
Title: ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST

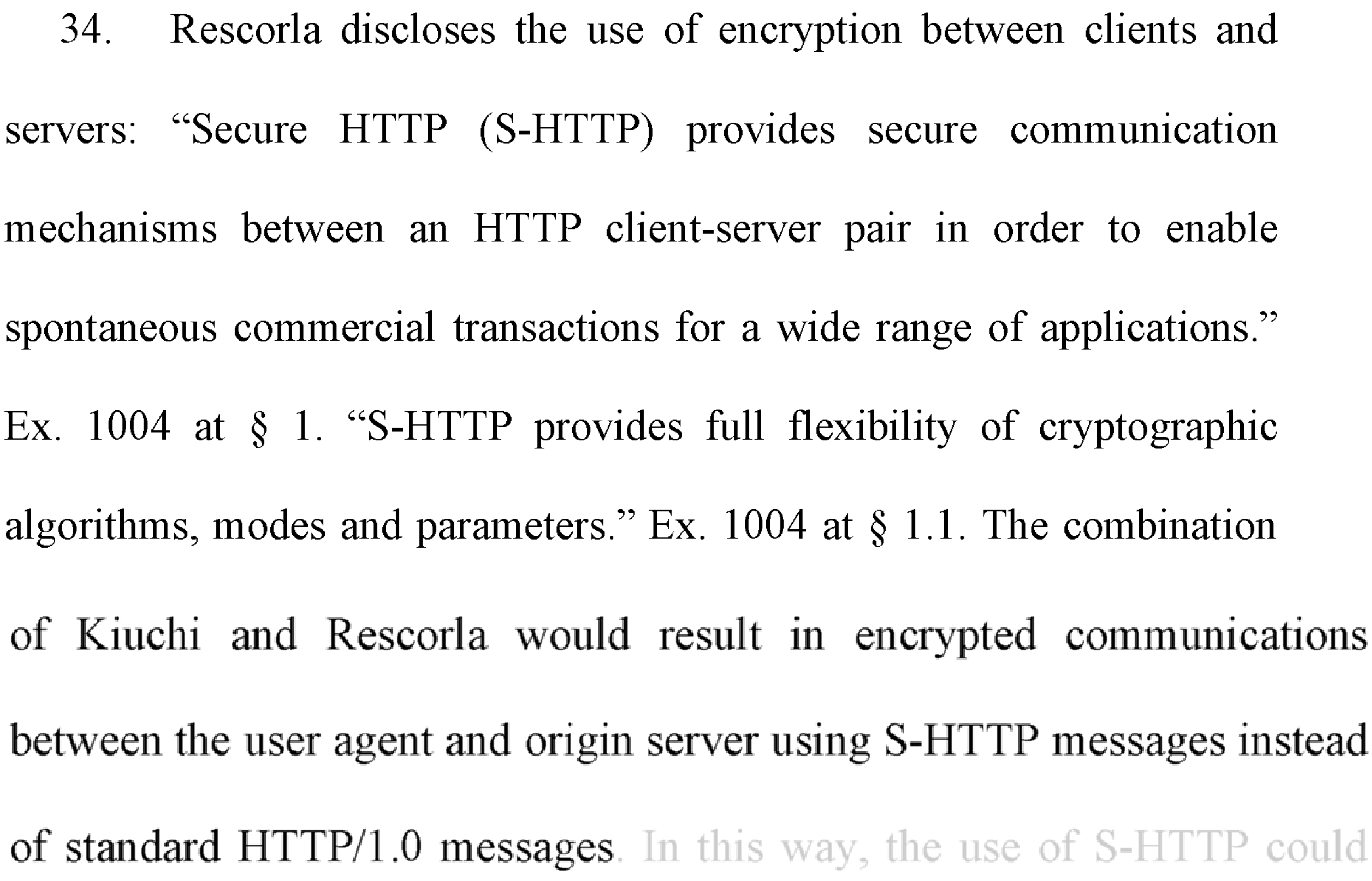
DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Science & Engineering department at Washington University in St. Louis. I have been asked to offer technical opinions relating to U.S. Patent No. 7,490,151, and prior art references relating to its subject matter. My current *curriculum vitae* is attached and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure des télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) and PhD (1986) in electrical engineering from The California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at the IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I was a research staff member within the Communication Department, where I worked to design and evaluate high-speed switches

Dr. Guerin



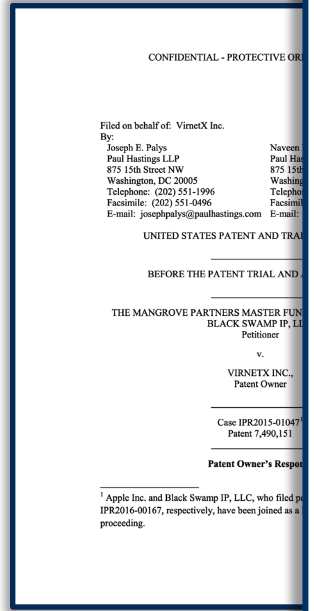
34. Rescorla discloses the use of encryption between clients and servers: "Secure HTTP (S-HTTP) provides secure communication mechanisms between an HTTP client-server pair in order to enable spontaneous commercial transactions for a wide range of applications." Ex. 1004 at § 1. "S-HTTP provides full flexibility of cryptographic algorithms, modes and parameters." Ex. 1004 at § 1.1. The combination of Kiuchi and Rescorla would result in encrypted communications between the user agent and origin server using S-HTTP messages instead of standard HTTP/1.0 messages. In this way, the use of S-HTTP could

Ex. 1003 at ¶34; Pet. (Paper 5) at 38-40

VirnetX Does Not Contest Rescorla Teaches End-to-End Encryption

151 Patent Owner Response (Paper 48)

Response
Paper 4



CONFIDENTIAL - PROTECTIVE OR

Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys | Naveen
Paul Hastings LLP | Paul Ha
875 15th Street NW | 875 15t
Washington, DC 20005 | Washing
Telephone: (202) 551-1996 | Telepho
Facsimile: (202) 551-0496 | Facsimil
E-mail: josephpalys@paulhastings.com | E-mail:

UNITED STATES PATENT AND TRA

BEFORE THE PATENT TRIAL AND

THE MANGROVE PARTNERS MASTER FUN
BLACK SWAMP IP, LL
Petitioner

v.

VIRNETX INC.,
Patent Owner

Case IPR2015-01047[1]
Patent 7,490,151

Patent Owner's Respon

[1] Apple Inc. and Black Swamp IP, LLC, who filed p
IPR2016-00167, respectively, have been joined as a
proceeding.

First, Kiuchi contains many deficiencies that Petitioners do not even allege are addressed by Rescorla or RFC 1034. (*See supra* Sections III.B-D.) For instance, Kiuchi does not disclose the claimed DNS features (*see supra* Section III.B.1), does not "determin[e] whether the intercepted DNS request corresponds to a secure server" (*see supra* Section III.B.2), and does not address the deficiencies discussed with respect to Petitioner Black Swamp in Section III.B.3.b. As such, for at least those reasons discussed above, Petitioners have failed to establish by a preponderance of the evidence that the claims are unpatentable in view of Kiuchi and Rescorla and/or RFC 1034. (Ex. 2038 at ¶¶ 62-63.)

151 PO Resp. at 28

The Federal Circuit Upheld Denial of JMOL

It Did Not Make Factual Findings on Kiuchi's Disclosure

VirnetX v. Cisco* *(Fed. Cir. 2014)

1308 767 FEDERAL REPORTER, 3d SERIES

incomplete that they could not be used without undue difficulty.

[10] Contrary to Mukand's argument, the deficiencies in its responses were not limited to a discrete category of information. As Commerce noted, Mukand assigned the "same amount of conversion costs per kilogram of bar produced, irrespective of the final size of the product produced." J.A. 1604. Mukand thus premised all of its production cost data on the assumption that product size is not a significant cost factor—an assumption it failed to support. In general, use of partial facts available is not appropriate when the missing information is core to the antidumping analysis and leaves little room for the substitution of partial facts without undue difficulty.[12] Without cost data broken down by product size, Commerce was unable to differentiate between different types of steel bar products and could not calculate an accurate constructed value for any of Mukand's products. We therefore hold that Commerce's reliance on total AFA is supported by substantial evidence.

III

For the reasons set forth above, we affirm the decision of the Trade Court.

AFFIRMED

[12] *See Shanghai Taoen Int'l Co. v. United States*, 360 F.Supp.2d 1339, 1348 n. 13 (Ct. Int'l Trade 2005).

VIRNETX, INC., Pla

and

Science Applications
Corporation, I
Appelle

v.

CISCO SYSTEMS, I

and

Apple Inc., Defenda

No. 2013-

United States Cou
Federal Ci

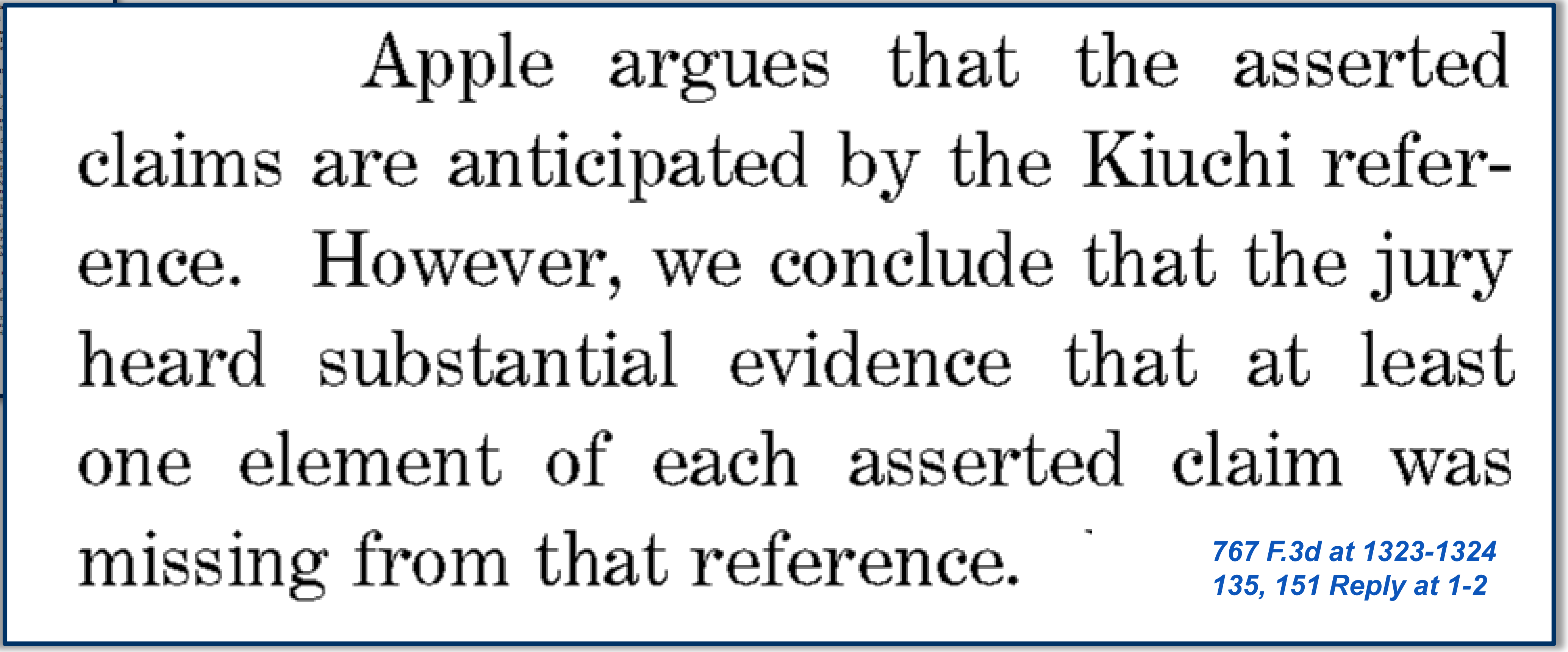
Sept. 16, 2

Background: Patente against mobile phone m ing infringement of p method of transparent private network (VPN computer and target com disclosing secure doma The United States Dist Eastern District of Tex Chief Judge, 2009 WL WL 3135639, construed then denied manufactur tions after jury returne tee's favor 925 F.Supp.2 er appealed.

Holdings: The Court Chief Judge, held that:

(1) term "domain name" responding to Inter address;

(2) term "secure com meant direct comm provided data securi

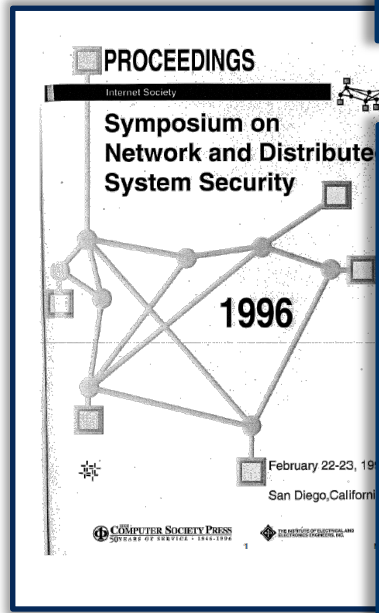


Apple argues that the asserted claims are anticipated by the Kiuchi reference. However, we conclude that the jury heard substantial evidence that at least one element of each asserted claim was missing from that reference.

767 F.3d at 1323-1324
135, 151 Reply at 1-2

Kiuchi

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

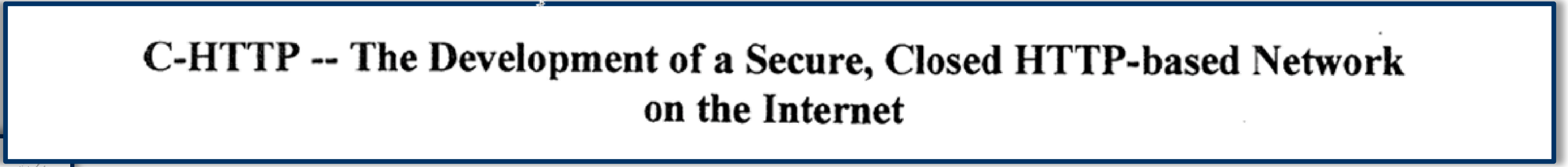
Symposium on
Network and Distribute
System Security

1996

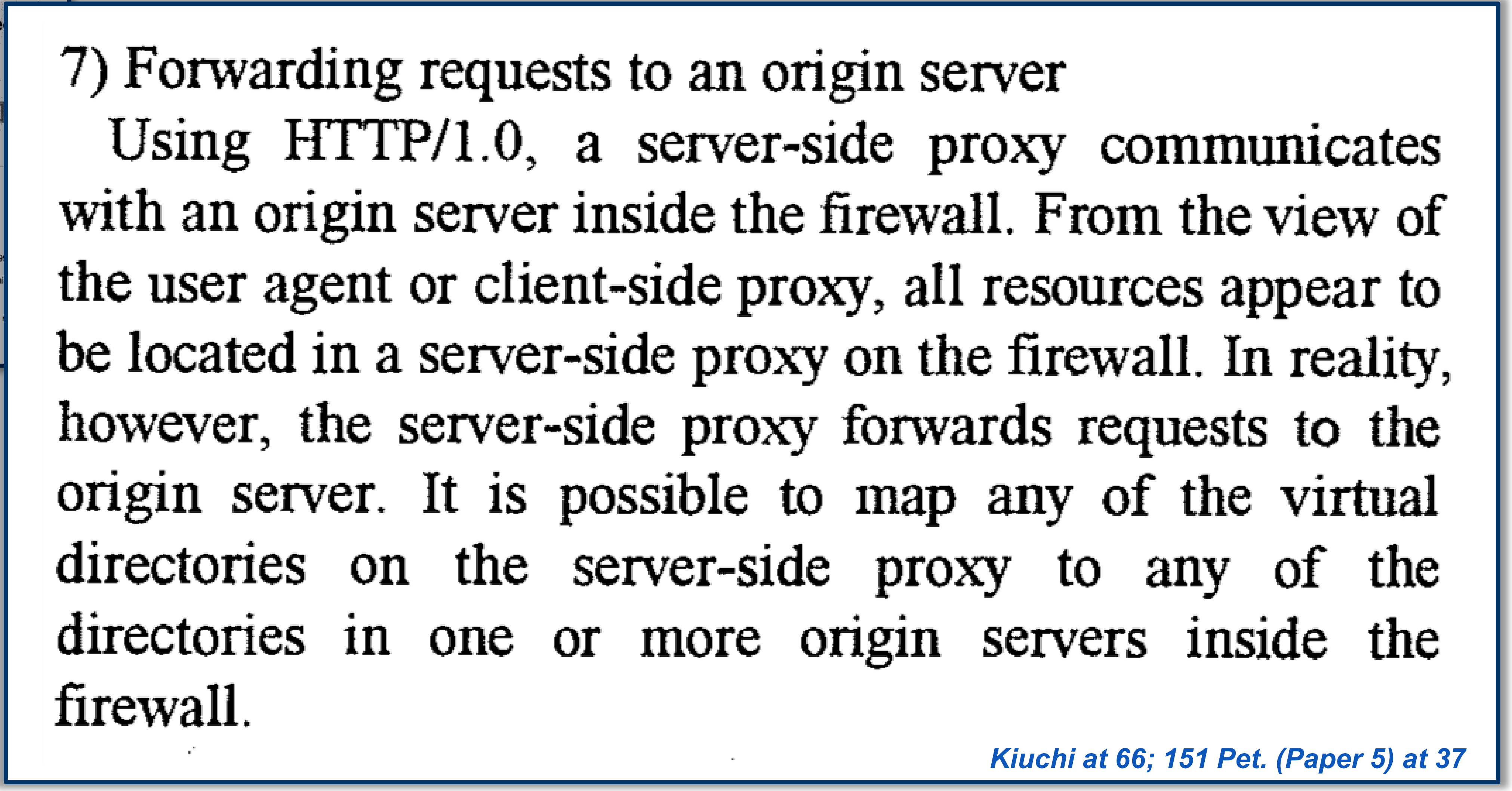
February 22-23, 19

San Diego,Californi

COMPUTER SOCIETY PRESS



C-HTTP -- The Development of a Secure, Closed HTTP-based Network
on the Internet



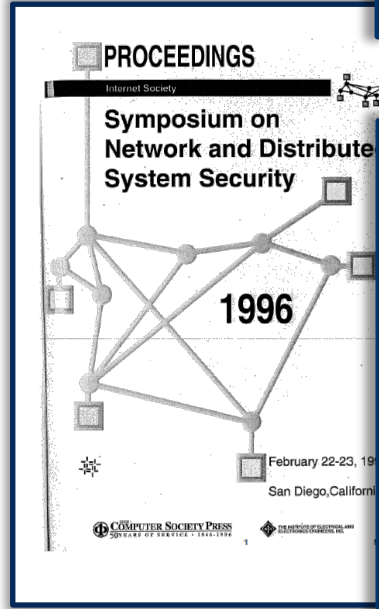
7) Forwarding requests to an origin server

Using HTTP/1.0, a server-side proxy communicates with an origin server inside the firewall. From the view of the user agent or client-side proxy, all resources appear to be located in a server-side proxy 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.

Kiuchi at 66; 151 Pet. (Paper 5) at 37

Kiuchi

Kiuchi
Ex. 1002



PROCEEDINGS

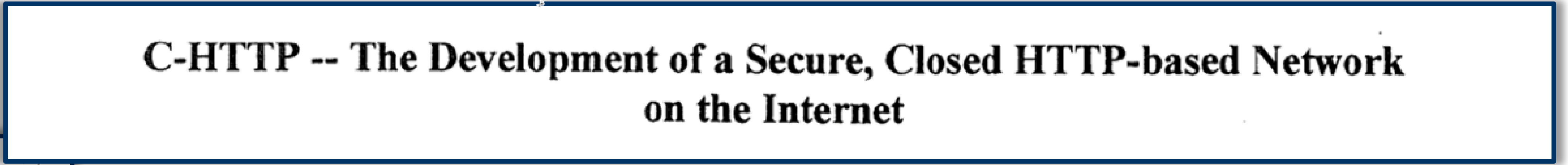
Internet Society

Symposium on
Network and Distribute
System Security

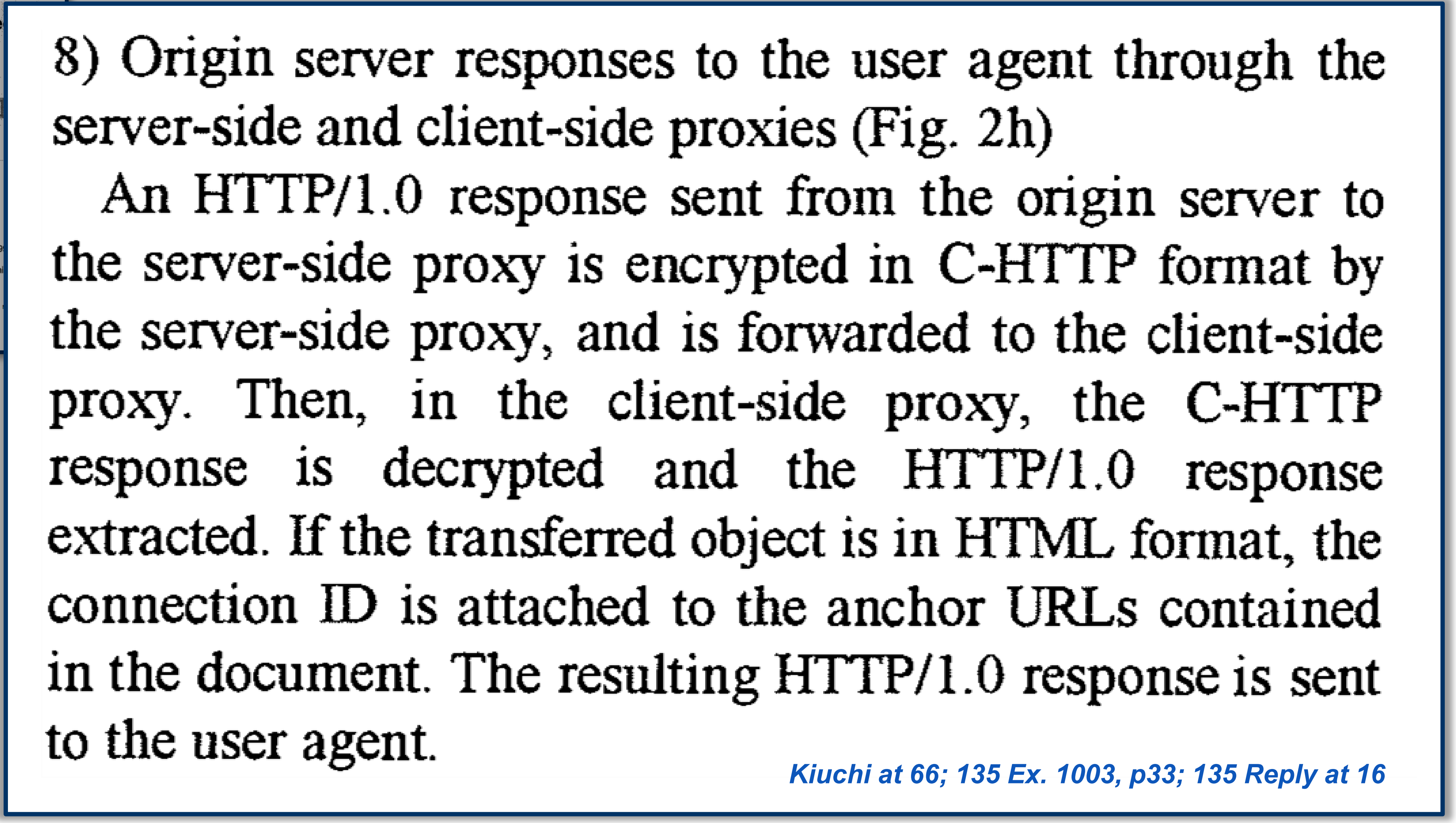
1996

February 22-23, 19

San Diego,Californ



C-HTTP -- The Development of a Secure, Closed HTTP-based Network
on the Internet



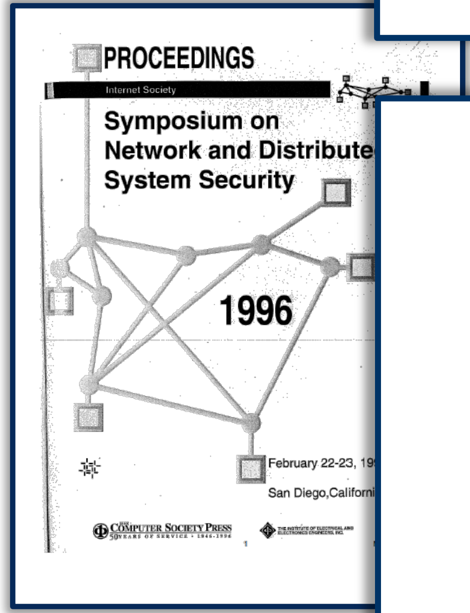
8) Origin server responses to the user agent through the server-side and client-side proxies (Fig. 2h)

An HTTP/1.0 response sent from the origin server to the server-side proxy is encrypted in C-HTTP format by the server-side proxy, and is forwarded to the client-side proxy. Then, in the client-side proxy, the C-HTTP response is decrypted and the HTTP/1.0 response extracted. If the transferred object is in HTML format, the connection ID is attached to the anchor URLs contained in the document. The resulting HTTP/1.0 response is sent to the user agent.

Kiuchi at 66; 135 Ex. 1003, p33; 135 Reply at 16

Kiuchi

Kiuchi
Ex. 1002



PROCEEDINGS
Internet Society
Symposium on
Network and Distribute
System Security
1996
February 22-23, 19
San Diego,Californi
COMPUTER SOCIETY PRESS

C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet

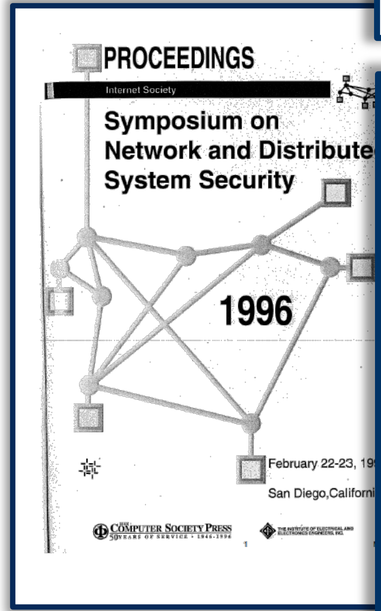
2) No simultaneous data transfer to both sides

Only after receiving all the data transferred from one side, does a proxy server begin to forward it to the other side, except for image and sound data. In this method, the performance of data transfer is not good, however, the data transfer is separated between the internal and external sides. For the secure implementation of this feature, the size of HTML documents and object bodies should be limited and checked by each proxy. We plan to implement routines which check the contents of object bodies (especially concerning form data used in POST method) in the future.

Kiuchi at 67; 135 Reply at 16

Kiuchi

Kiuchi
Ex. 1002



PROCEEDINGS

Internet Society

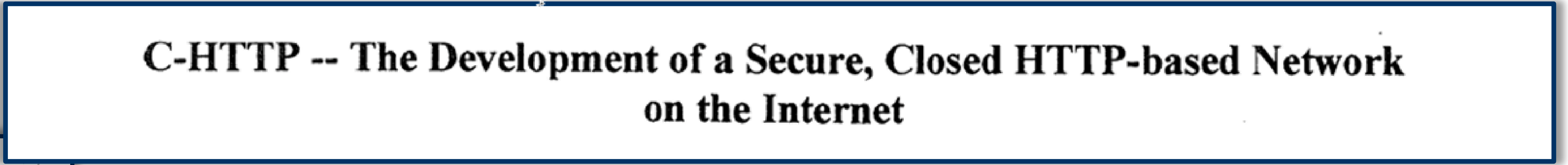
Symposium on
Network and Distribute
System Security

1996

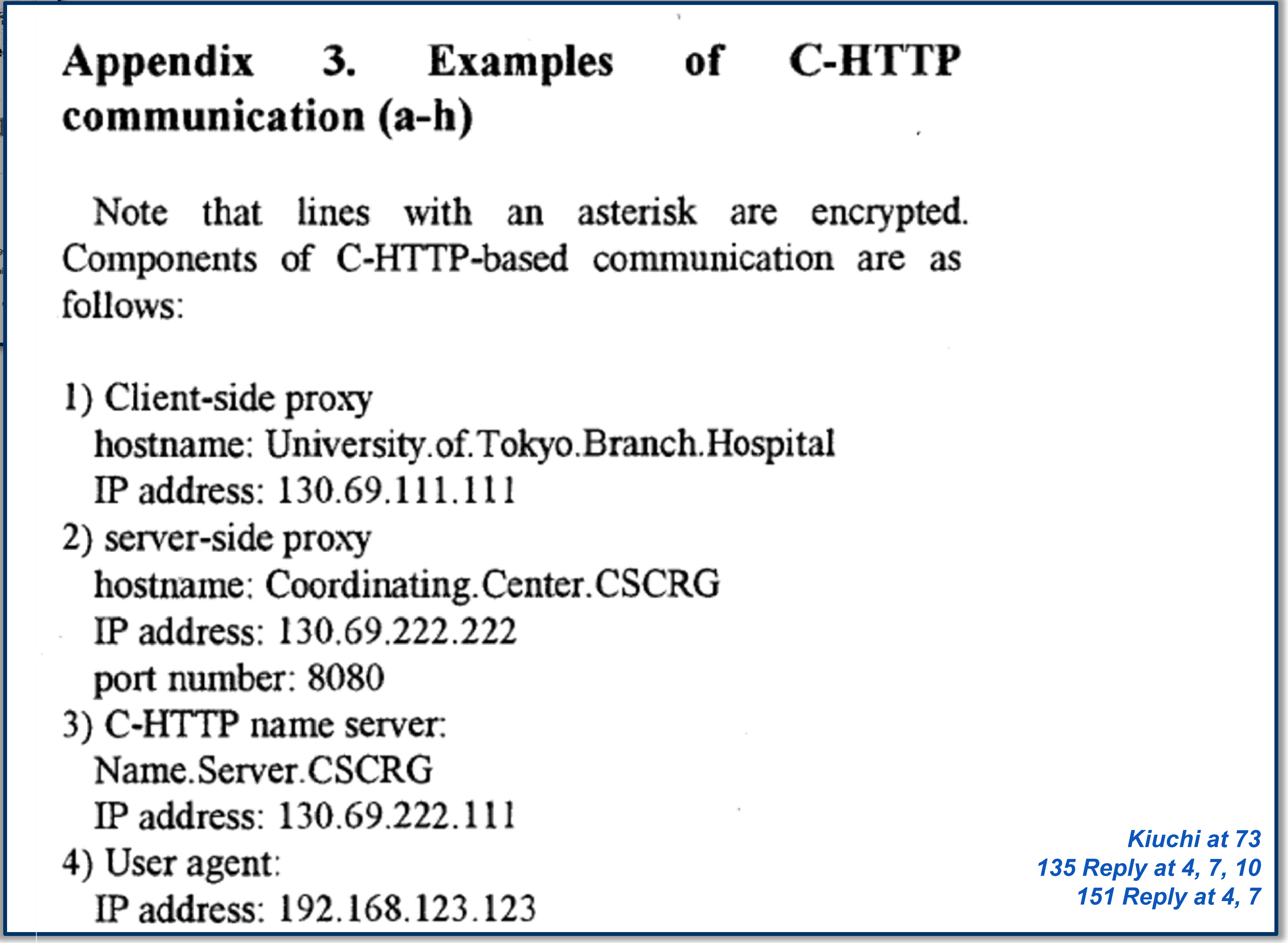
February 22-23, 19

San Diego,Californi

Computer Society Press



C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet



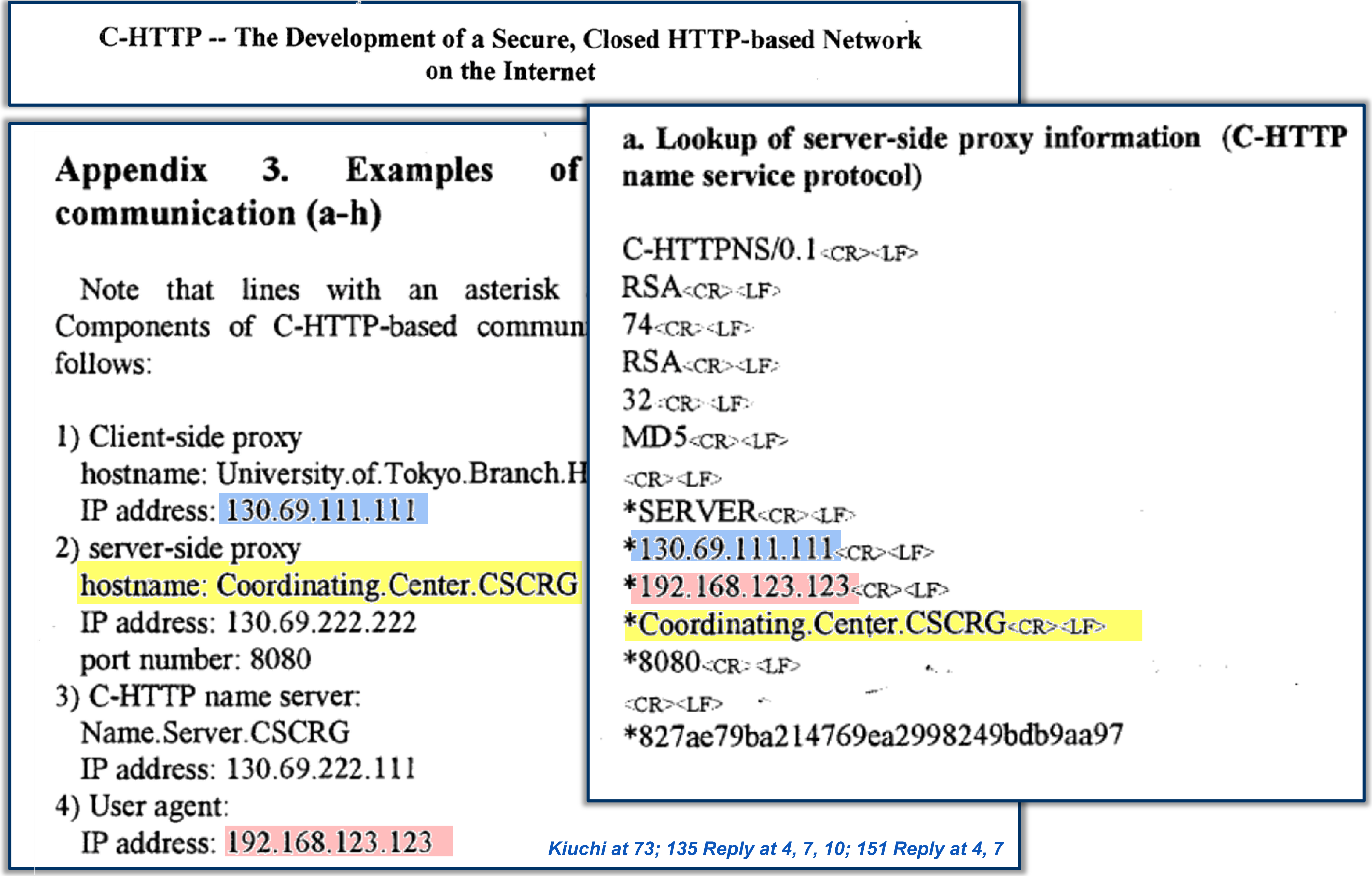
Appendix 3. Examples of C-HTTP communication (a-h)

Note that lines with an asterisk are encrypted. Components of C-HTTP-based communication are as follows:

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
3) C-HTTP name server:
   Name.Server.CSCRG
   IP address: 130.69.222.111
4) User agent:
   IP address: 192.168.123.123

Kiuchi at 73
135 Reply at 4, 7, 10
151 Reply at 4, 7

Kiuchi



C-HTTP -- The Development of a Secure, Closed HTTP-based Network
on the Internet

Appendix 3. Examples of
communication (a-h)

Note that lines with an asterisk
Components of C-HTTP-based commun
follows:

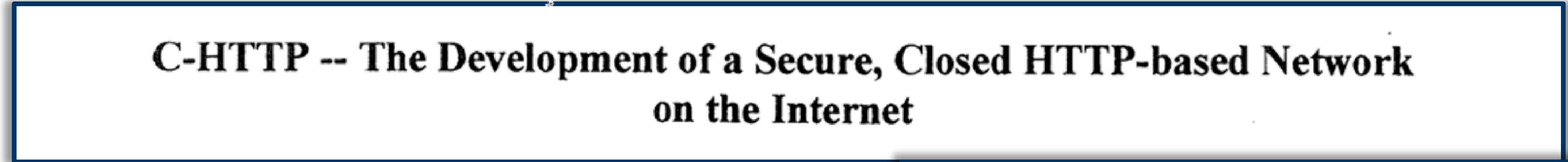
1) Client-side proxy
   hostname: University.of.Tokyo.Branch.H
   IP address: 130.69.111.111
2) server-side proxy
   hostname: Coordinating.Center.CSCRG
   IP address: 130.69.222.222
   port number: 8080
3) C-HTTP name server:
   Name.Server.CSCRG
   IP address: 130.69.222.111
4) User agent:
   IP address: 192.168.123.123

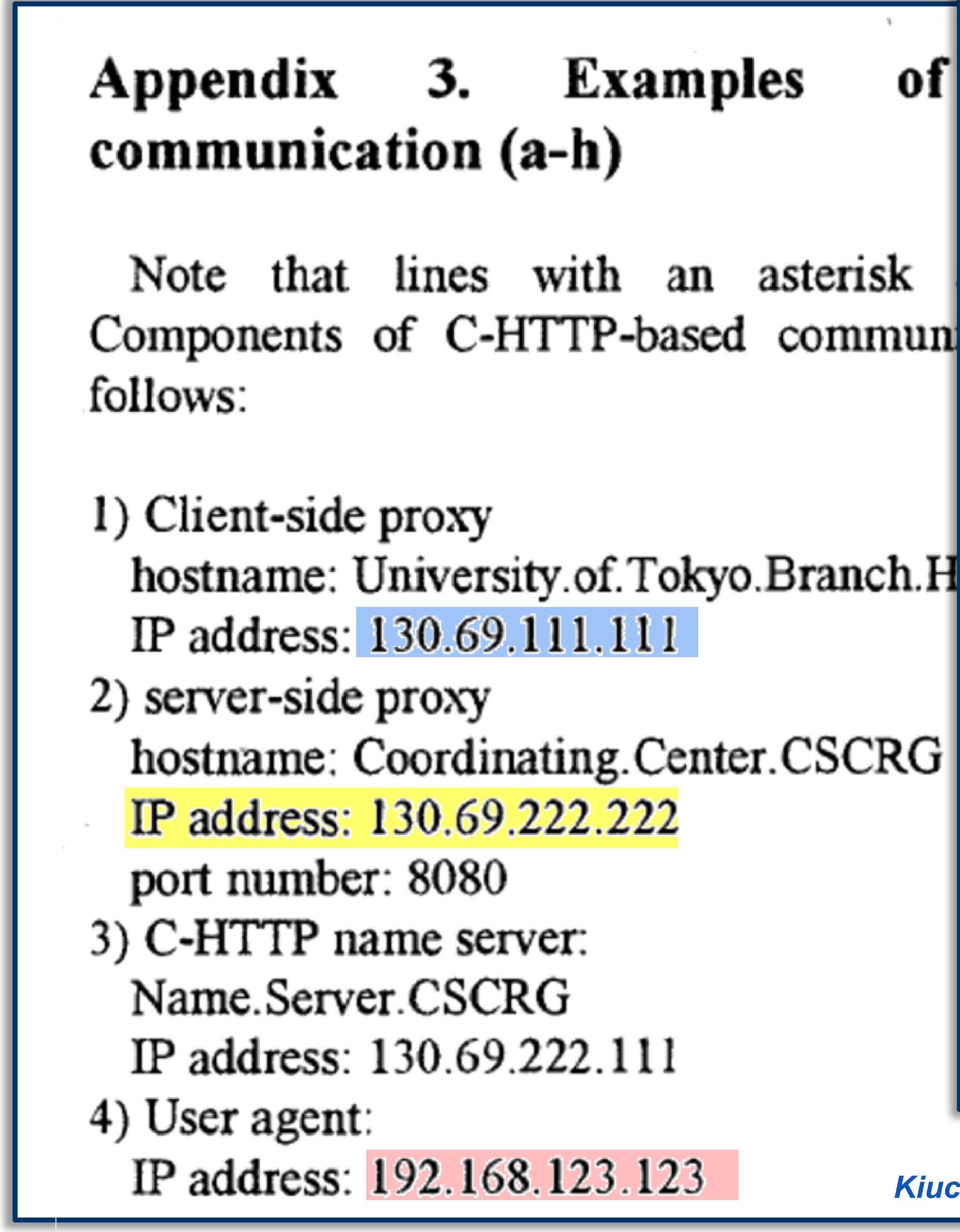
a. Lookup of server-side proxy information (C-HTTP name service protocol)

```
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
```

Kiuchi at 73; 135 Reply at 4, 7, 10; 151 Reply at 4, 7

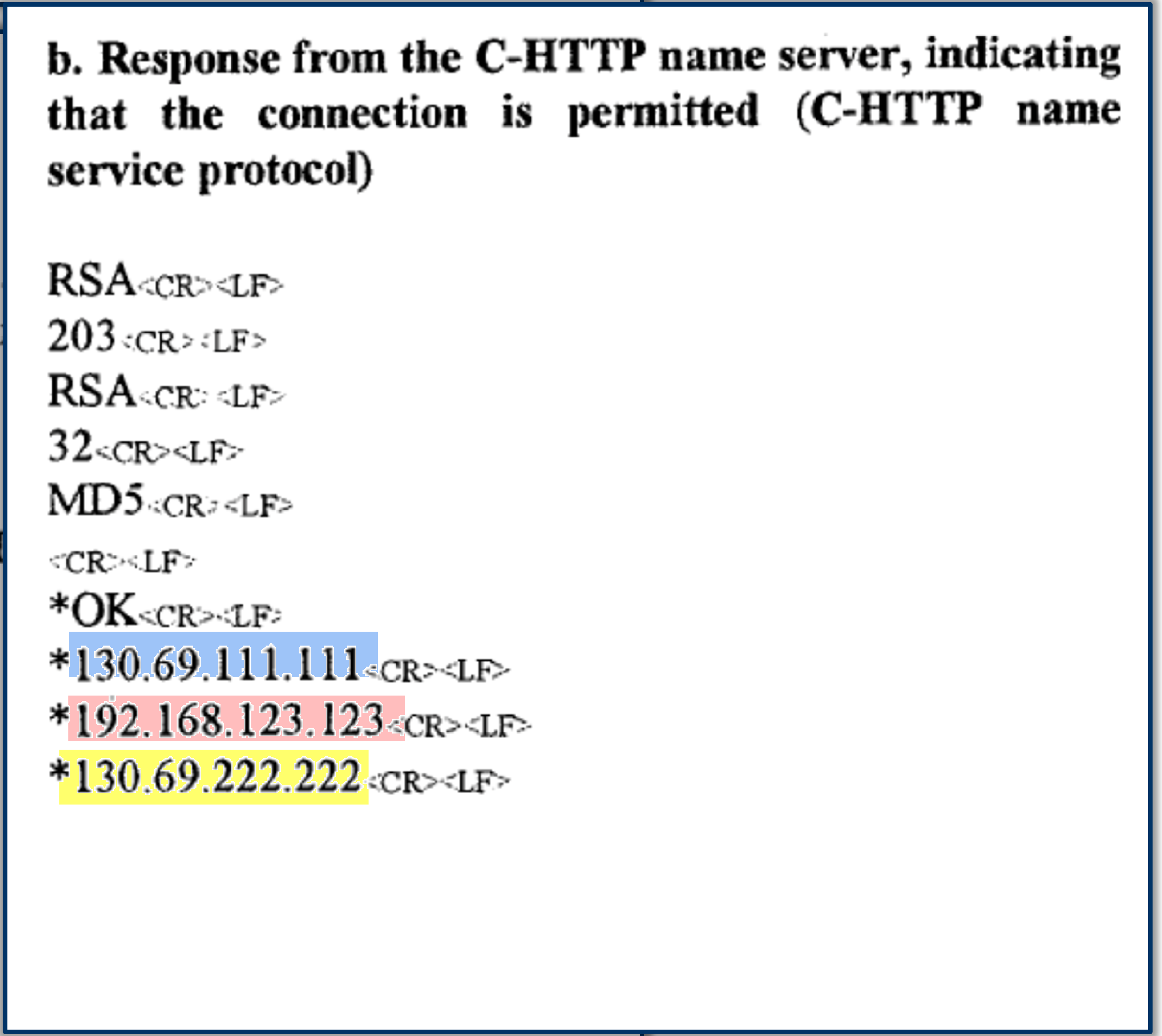
Kiuchi


C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet


Appendix 3. Examples of communication (a-h)

Note that lines with an asterisk Components of C-HTTP-based commun follows:

1) Client-side proxy
hostname: University.of.Tokyo.Branch.H
IP address: 130.69.111.111
2) server-side proxy
hostname: Coordinating.Center.CSCRG
IP address: 130.69.222.222
port number: 8080
3) C-HTTP name server:
Name.Server.CSCRG
IP address: 130.69.222.111
4) User agent:
IP address: 192.168.123.123

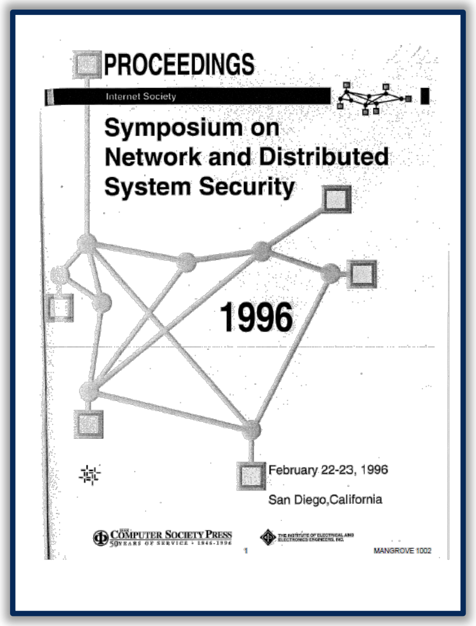

b. Response from the C-HTTP name server, indicating that the connection is permitted (C-HTTP name service protocol)

```
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>
```

Kiuchi at 73; 135 Reply at 4, 7, 10; 151 Reply at 4, 7

Kiuchi

Kiuchi
Ex. 1002



PROCEEDINGS

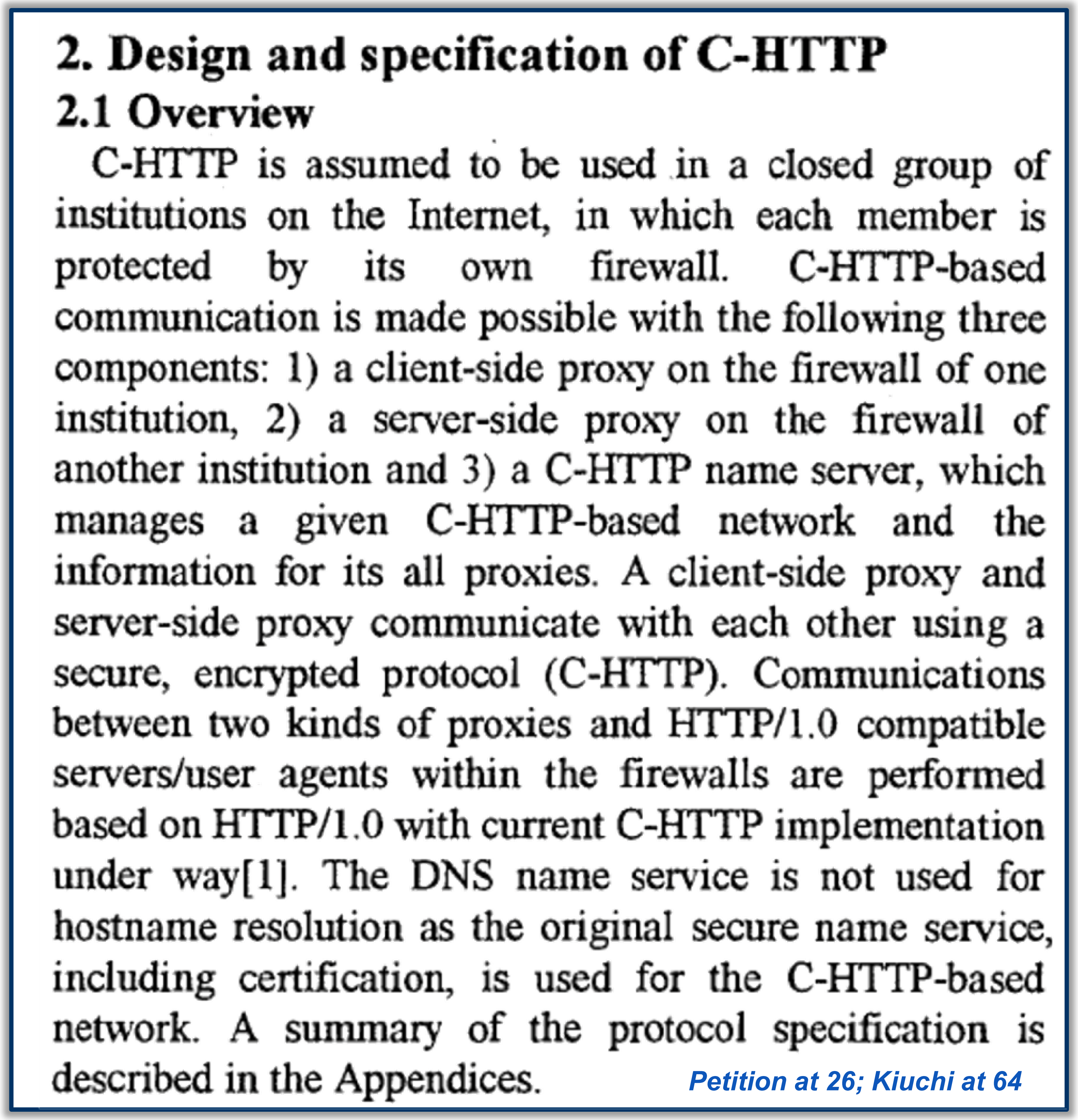
Internet Society

Symposium on
Network and Distributed
System Security

1996

February 22-23, 1996

San Diego,California



2. Design and specification of C-HTTP

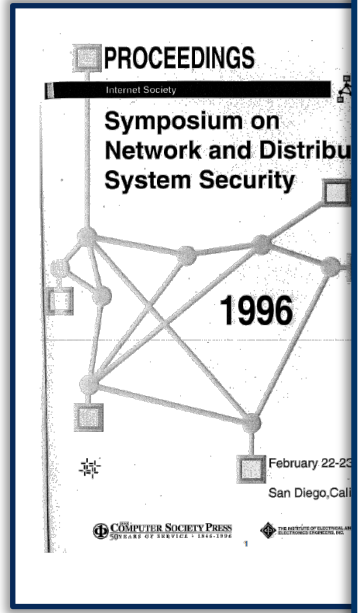
2.1 Overview

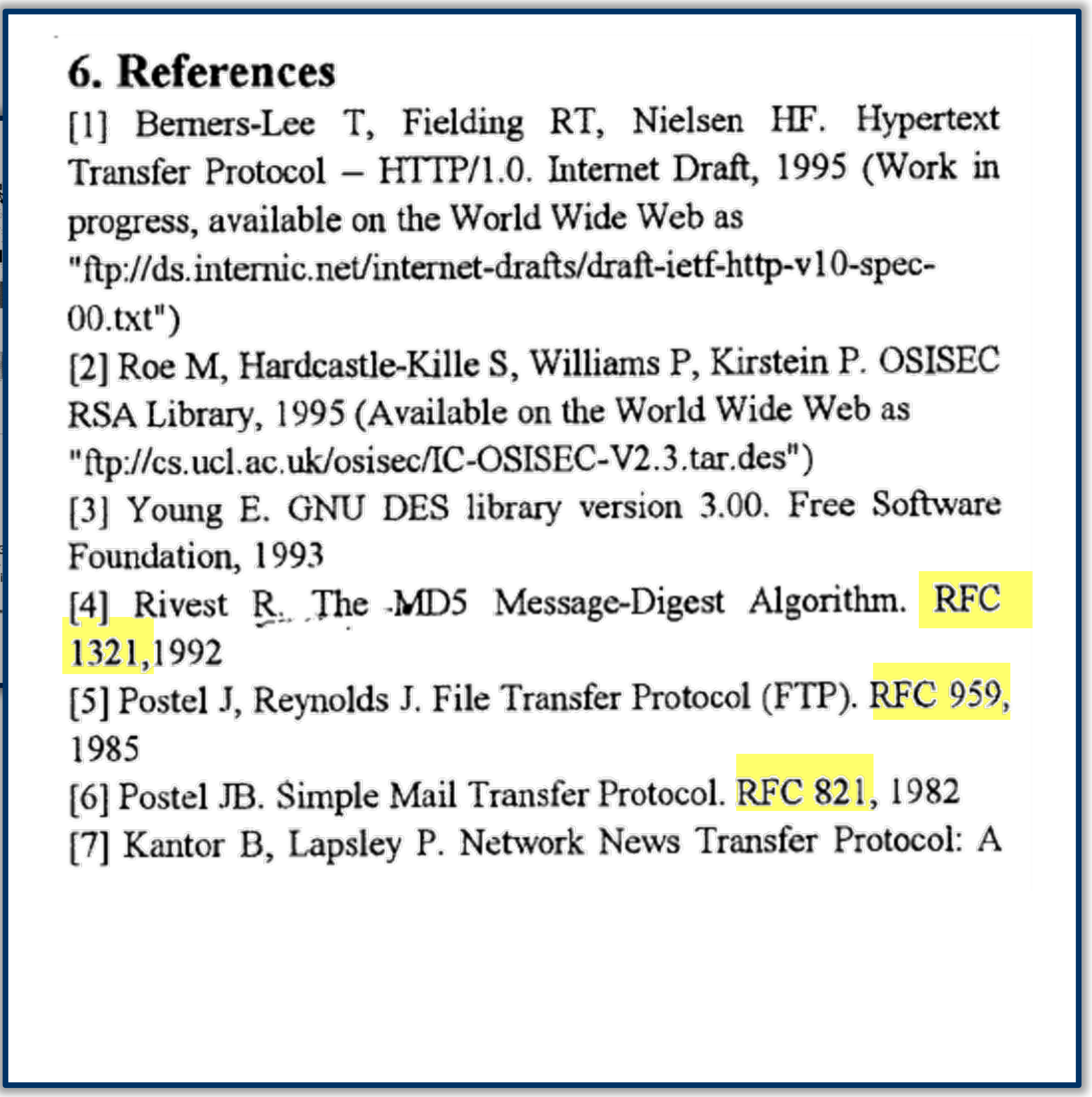
C-HTTP is assumed to be used in a closed group of institutions on the Internet, in which each member is protected by its own firewall. C-HTTP-based communication is made possible with the following three components: 1) a client-side proxy on the firewall of one institution, 2) a server-side proxy on the firewall of another institution and 3) a C-HTTP name server, which manages a given C-HTTP-based network and the information for its all proxies. A client-side proxy and server-side proxy communicate with each other using a secure, encrypted protocol (C-HTTP). Communications between two kinds of proxies and HTTP/1.0 compatible servers/user agents within the firewalls are performed based on HTTP/1.0 with current C-HTTP implementation under way[1]. 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. A summary of the protocol specification is described in the Appendices.

Petition at 26; Kiuchi at 64

Kiuchi

Kiuchi
Ex. 1002





6. References

[1] Berners-Lee T, Fielding RT, Nielsen HF. Hypertext Transfer Protocol – HTTP/1.0. Internet Draft, 1995 (Work in progress, available on the World Wide Web as "ftp://ds.internic.net/internet-drafts/draft-ietf-http-v10-spec-00.txt")

[2] Roe M, Hardcastle-Kille S, Williams P, Kirstein P. OSISEC RSA Library, 1995 (Available on the World Wide Web as "ftp://cs.ucl.ac.uk/osisec/IC-OSISEC-V2.3.tar.des")

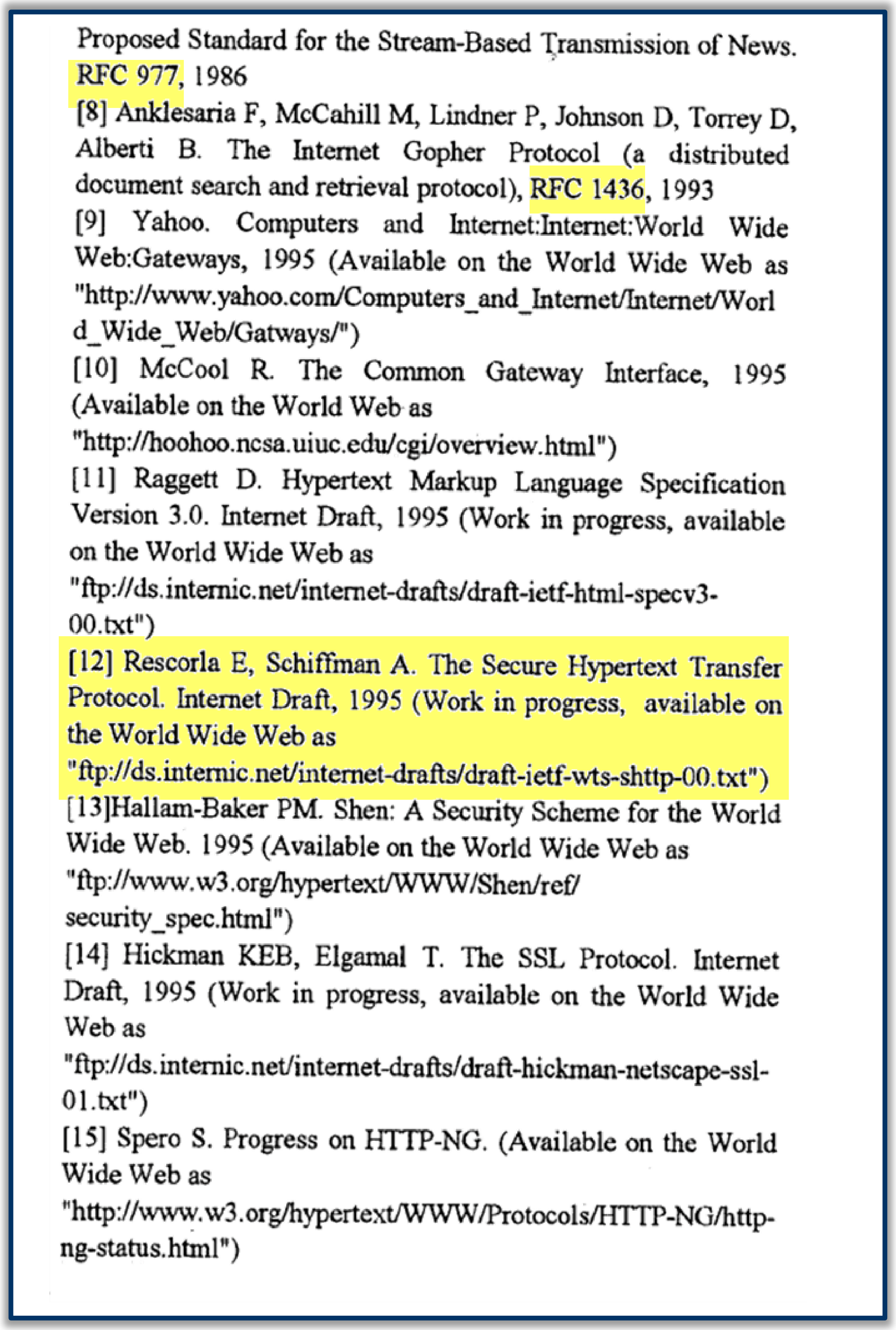
[3] Young E. GNU DES library version 3.00. Free Software Foundation, 1993

[4] Rivest R. The MD5 Message-Digest Algorithm. RFC 1321,1992

[5] Postel J, Reynolds J. File Transfer Protocol (FTP). RFC 959, 1985

[6] Postel JB. Simple Mail Transfer Protocol. RFC 821, 1982

[7] Kantor B, Lapsley P. Network News Transfer Protocol: A



Proposed Standard for the Stream-Based Transmission of News. RFC 977, 1986

[8] Anklesaria F, McCahill M, Lindner P, Johnson D, Torrey D, Alberti B. The Internet Gopher Protocol (a distributed document search and retrieval protocol), RFC 1436, 1993

[9] Yahoo. Computers and Internet:Internet:World Wide Web:Gateways, 1995 (Available on the World Wide Web as "http://www.yahoo.com/Computers_and_Internet/Internet/World_Wide_Web/Gatways/")

[10] McCool R. The Common Gateway Interface, 1995 (Available on the World Web as "http://hoohoo.ncsa.uiuc.edu/cgi/overview.html")

[11] Raggett D. Hypertext Markup Language Specification Version 3.0. Internet Draft, 1995 (Work in progress, available on the World Wide Web as "ftp://ds.internic.net/internet-drafts/draft-ietf-html-specv3-00.txt")

[12] Rescorla E, Schiffman A. The Secure Hypertext Transfer Protocol. Internet Draft, 1995 (Work in progress, available on the World Wide Web as "ftp://ds.internic.net/internet-drafts/draft-ietf-wts-shttp-00.txt")

[13]Hallam-Baker PM. Shen: A Security Scheme for the World Wide Web. 1995 (Available on the World Wide Web as "ftp://www.w3.org/hypertext/WWW/Shen/ref/security_spec.html")

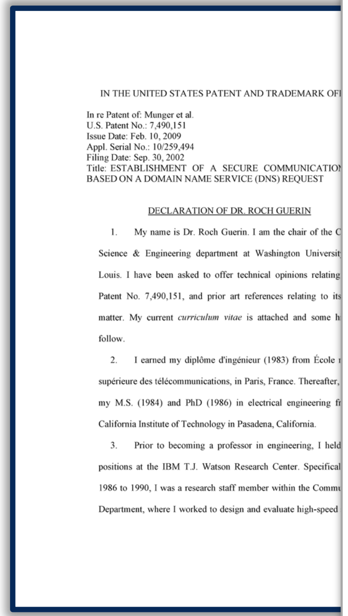
[14] Hickman KEB, Elgamal T. The SSL Protocol. Internet Draft, 1995 (Work in progress, available on the World Wide Web as "ftp://ds.internic.net/internet-drafts/draft-hickman-netscape-ssl-01.txt")

[15] Spero S. Progress on HTTP-NG. (Available on the World Wide Web as "http://www.w3.org/hypertext/WWW/Protocols/HTTP-NG/http-ng-status.html")

Kiuchi at 69-70
135 Reply at 21
151 Reply at 19-20

RFCs

Dr. Guerin
Ex. 1003



IN THE UNITED STATES PATENT AND TRADEMARK OFI

In re Patent of: Munger et al.
U.S. Patent No.: 7,490,151
Issue Date: Feb. 10, 2009
Appl. Serial No.: 10/259,494
Filing Date: Sep. 30, 2002
Title: ESTABLISHMENT OF A SECURE COMMUNICATION
BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the C
Science & Engineering department at Washington Universit
Louis. I have been asked to offer technical opinions relating
Patent No. 7,490,151, and prior art references relating to its
matter. My current *curriculum vitae* is attached and some h
follow.

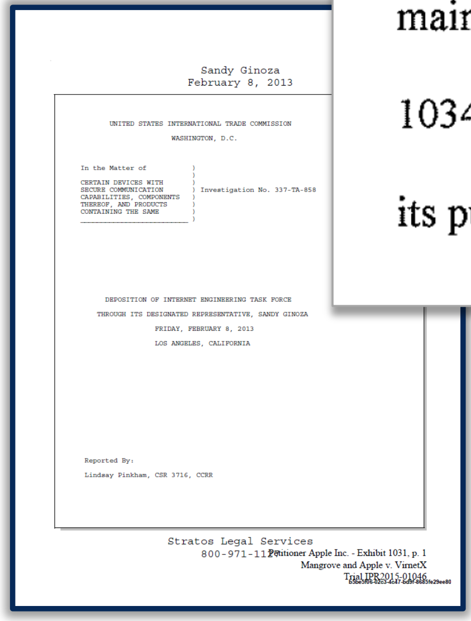
2. I earned my diplôme d'ingénieur (1983) from École r
supérieure des télécommunications, in Paris, France. Thereafter,
my M.S. (1984) and PhD (1986) in electrical engineering fr
California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held
positions at the IBM T.J. Watson Research Center. Specifical
1986 to 1990, I was a research staff member within the Commu
Department, where I worked to design and evaluate high-speed

44. RFC documents are published on a specific date, which starts a period for others to provide comments on the document. Ex.1010, pp. 19-20 (§ 6.2) ("These minimum periods are intended to ensure adequate opportunity for community review without severely impacting timeliness. These intervals shall be measured from the date of publication of the corresponding RFC(s)…"). The publication date of each RFC is contained in the RFC, typically in the top right corner of the first page of the document. This is the date it was released for public distribution on the Internet.

135 Ex. 1003, ¶44; see 151 Ex. 1003, ¶48

Ginoza
Ex. 1031



Sandy Ginoza
February 8, 2013

UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, D.C.

```
In the Matter of            )
                            )
CERTAIN DEVICES WITH        )
SECURE COMMUNICATION        ) Investigation No. 337-TA-858
CAPABILITIES, COMPONENTS    )
THEREOF, AND PRODUCTS       )
CONTAINING THE SAME         )
___________________________ )
```

DEPOSITION OF INTERNET ENGINEERING TASK FORCE
THROUGH ITS DESIGNATED REPRESENTATIVE, SANDY GINOZA
FRIDAY, FEBRUARY 8, 2013
LOS ANGELES, CALIFORNIA

Reported By:
Lindsay Pinkham, CSR 3716, CCRR

Stratos Legal Services
800-971-1127

Petitioner Apple Inc. - Exhibit 1031, p. 1
Mangrove and Apple v. VirnetX
Trial IPR2015-01046
b5be5f06-02c3-4c47-bd9f-8685fe29ee80

11. Based on a search of RFC Editor records, I have determined that the RFC Editor maintained a copy of RFC 1034 in the ordinary course of its regularly conducted activities. RFC 1034 has been publicly available through the RFC Editor's web site or through other means since its publication in November 1987.

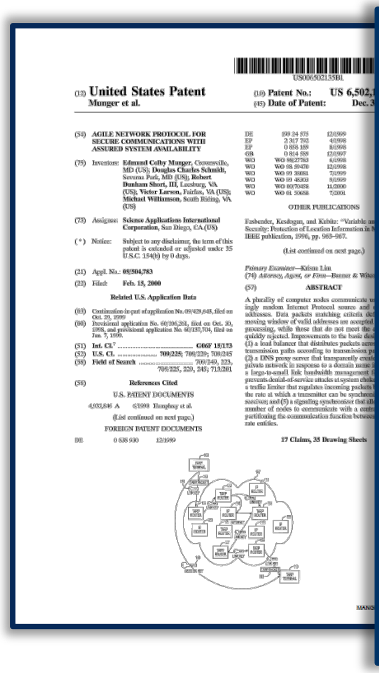
Ex. 1029 at ¶11

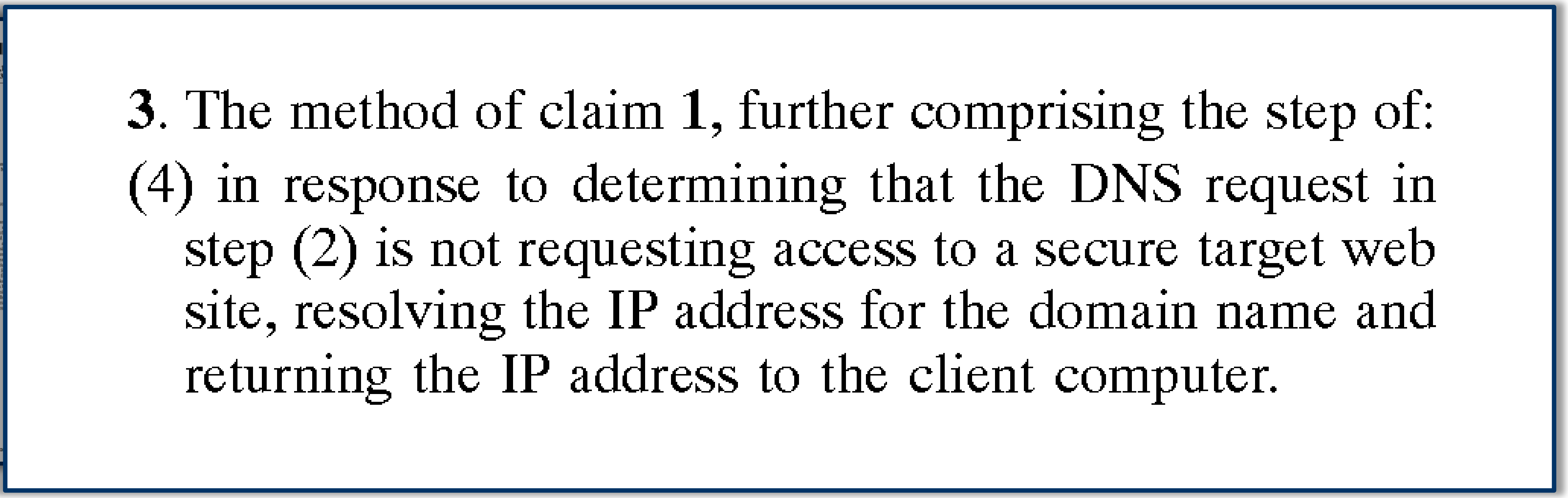
Q And you understand that you're here today testifying on behalf of the Internet Engineering Task Force?
A Yes.
Q And that your answers are given on behalf of the IETF?
A Yes.

Ex. 1031 at 10:5-11

135 Patent: Claims 3 and 8

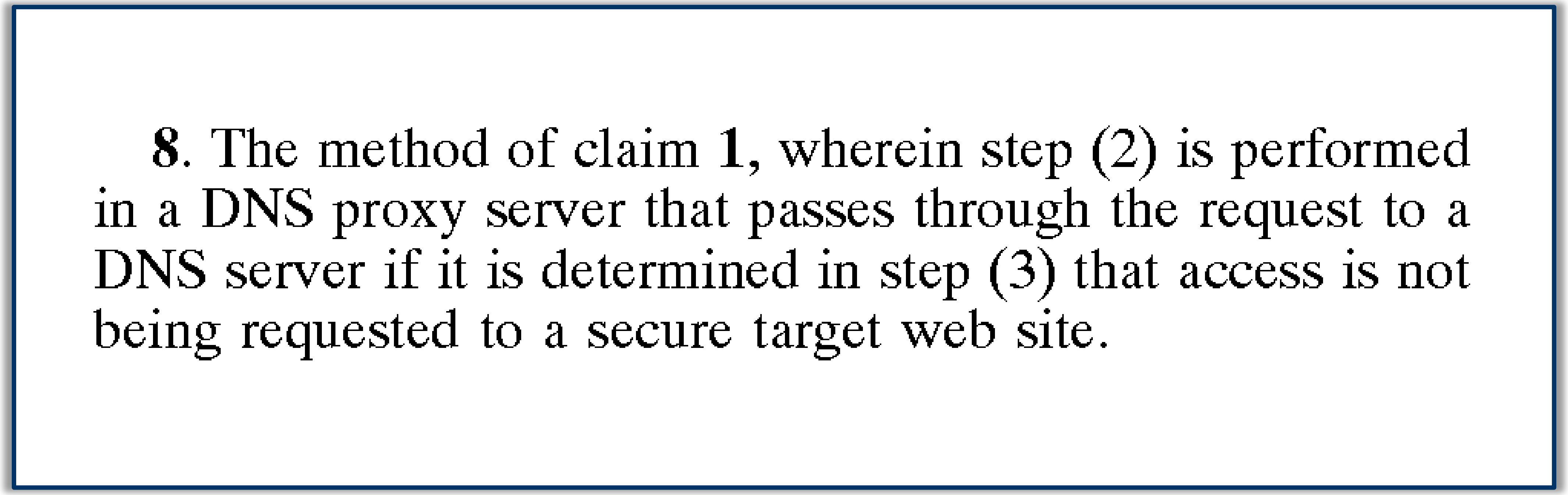
135 Patent
Ex. 1001





3. The method of claim 1, further comprising the step of:

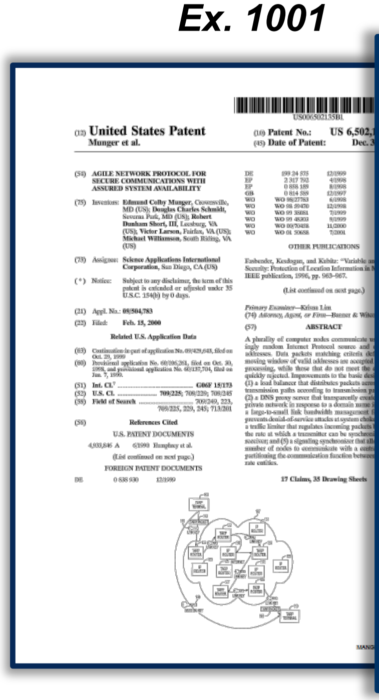
(4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer.



8. The method of claim 1, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site.

135 Patent: Claims 4 and 12

135 Patent
Ex. 1001



US006502135B1

(12) United States Patent
Munger et al.

(10) Patent No.: US 6,502,1
(45) Date of Patent: Dec. 3

(54) AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

(75) Inventors: Edmund Colby Munger, Crownsville, MD (US); Douglas Charles Schmidt, Severna Park, MD (US); Robert Dunham Short, III, Leesburg, VA (US); Victor Larson, Fairfax, VA (US); Michael Williamson, South Riding, VA (US)

(73) Assignee: Science Applications International Corporation, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/504,783

(22) Filed: Feb. 15, 2000

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, and provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) Int. Cl.^{7} G06F 15/173

(52) U.S. Cl. 709/225; 709/229; 709/245

(58) Field of Search 709/249, 223, 709/225, 229, 245; 713/201

(56) References Cited

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

DE 0 838 930 12/1999

DE	199 24 575	12/1999
EP	2 317 792	4/1998
EP	0 858 189	8/1998
GB	0 814 589	12/1997
WO	WO 98/27783	6/1998
WO	WO 98 59470	12/1998
WO	WO 99 38081	7/1999
WO	WO 99 48303	9/1999
WO	WO 00/70458	11/2000
WO	WO 01 50688	7/2001

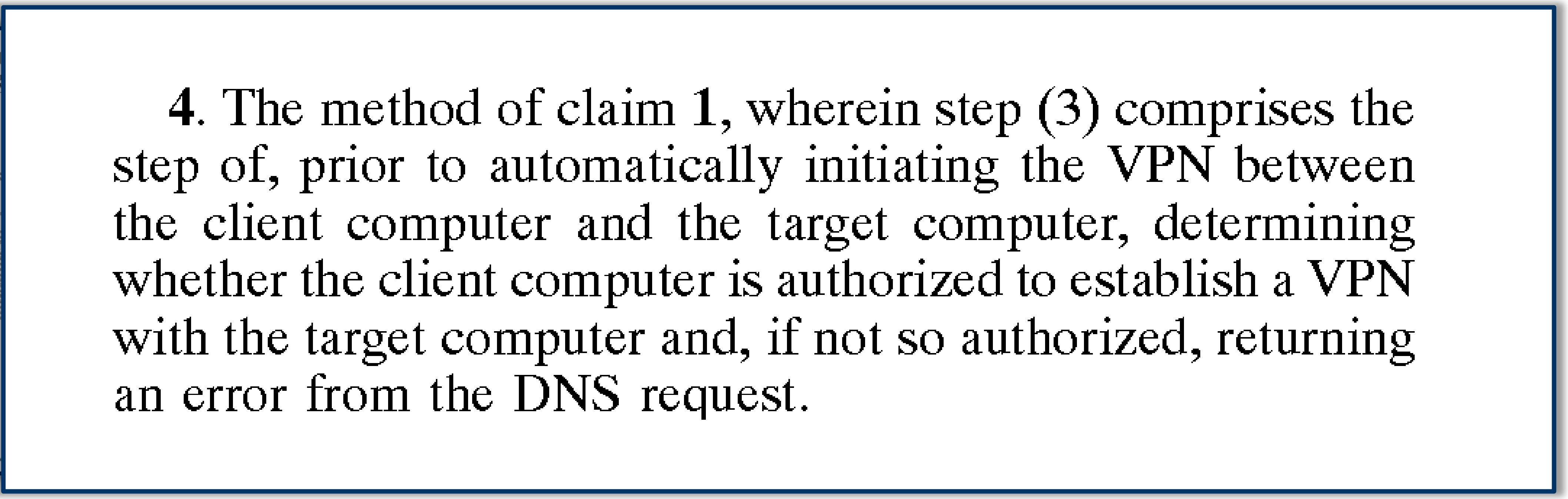
OTHER PUBLICATIONS

(List continued on next page.)

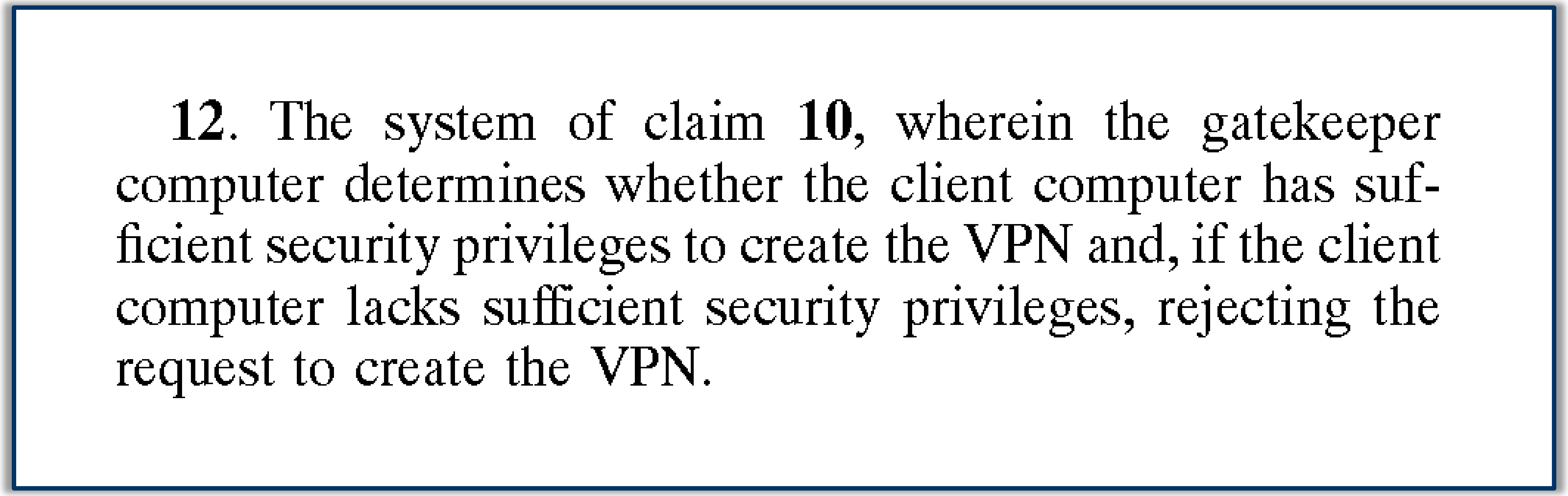
Primary Examiner—Krisna Lim

(57) ABSTRACT

17 Claims, 35 Drawing Sheets



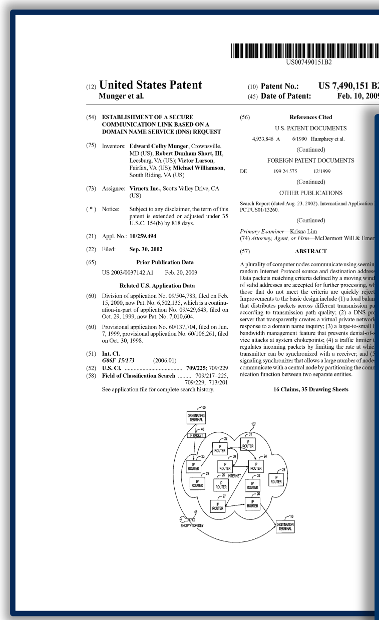
4. The method of claim **1**, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request.

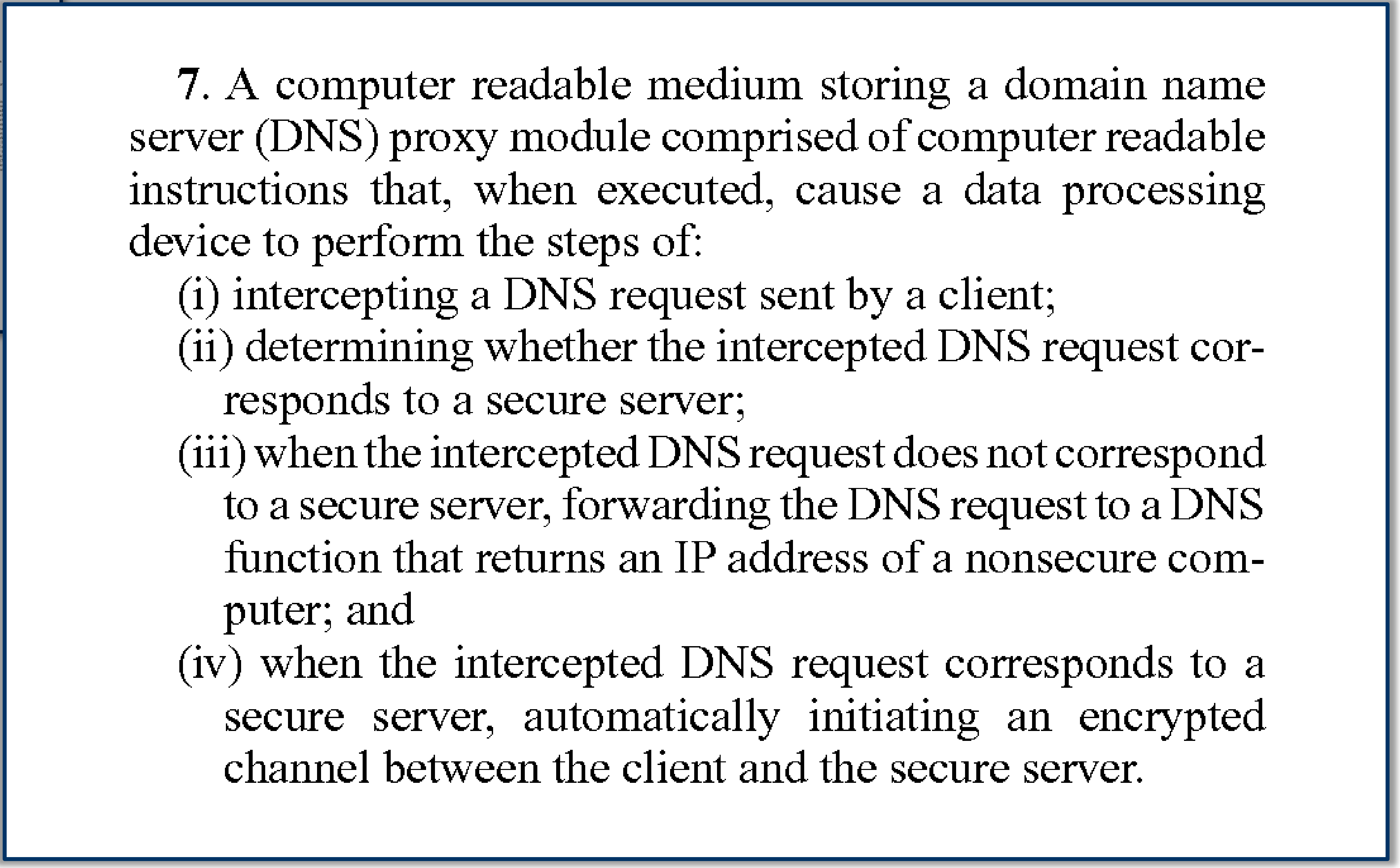


12. The system of claim **10**, wherein the gatekeeper computer determines whether the client computer has sufficient security privileges to create the VPN and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN.

151 Patent: Claim 7

151 Patent
Ex. 1001


United States Patent
Munger et al.
Patent No.: US 7,490,151 B2
Date of Patent: Feb. 10, 2009


7. A computer readable medium storing a domain name server (DNS) proxy module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) intercepting a DNS request sent by a client;

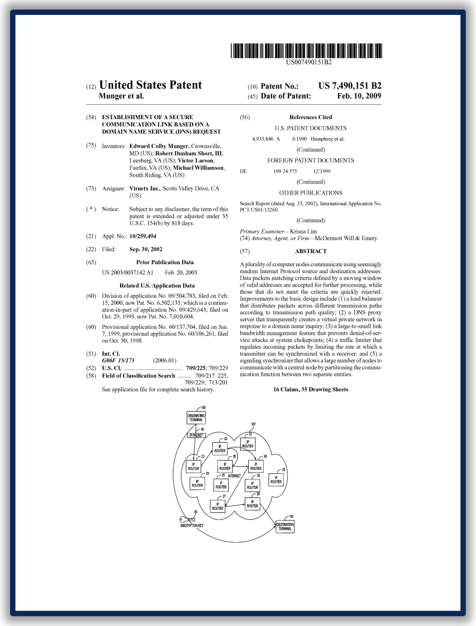
(ii) determining whether the intercepted DNS request corresponds to a secure server;

(iii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iv) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.

151 Patent: Claims 2, 8, 14

151 Patent
Ex. 1001



US007490151B2

(12) **United States Patent**
Munger et al.

(10) **Patent No.:** **US 7,490,151 B2**
(45) **Date of Patent:** **Feb. 10, 2009**

(54) **ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST**

(75) Inventors: **Edward Colby Munger**, Crownsville, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/259,494**

(22) Filed: **Sep. 30, 2002**

(65) **Prior Publication Data**

US 2003/0037142 A1 Feb. 20, 2003

Related U.S. Application Data

(60) Division 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.** **709/225**; 709/229
(58) **Field of Classification Search** 709/217–225, 709/229; 713/201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

(Continued)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emery

(57) **ABSTRACT**

A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design 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.

16 Claims, 35 Drawing Sheets

2. The data processing device of claim **1**, wherein step (iii) comprises the steps of:

(a) determining whether the client is authorized to access the secure server; and

(b) when the client is authorized to access the secure server, sending a request to the secure server to establish an encrypted channel between the secure server and the client.

8. The computer readable medium of claim **7**, wherein step (iv) comprises the steps of

(a) determining whether the client is authorized to access the secure server, and

(b) when the client is authorized to access the secure server, sending a request to the secure sewer to establish an encrypted channel between the secure sewer and the client.

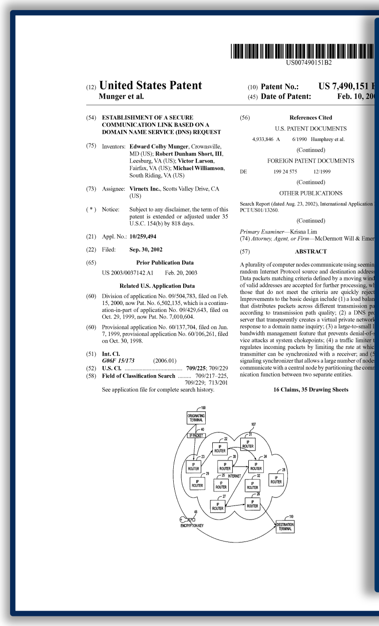
14. The computer readable medium of claim **13**, wherein step (iii) comprises the steps of

(a) determining whether the client is authorized to access the secure server; and

(b) when the client is authorized to access the secure server, sending a request to the secure server to establish a secure channel between the secure server and the client.

151 Patent: Clams 6 and 12

151 Patent
Ex. 1001



US007490151B2

(12) **United States Patent**
Munger et al.

(10) **Patent No.:** **US 7,490,151**
(45) **Date of Patent:** **Feb. 10, 20**

(54) **ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST**

(75) Inventors: **Edward Colby Munger**, Crownsville, MD (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Victor Larson**, Fairfax, VA (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virnetx Inc.**, Scotts Valley Drive, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/259,494**

(22) Filed: **Sep. 30, 2002**

(65) **Prior Publication Data**

US 2003/0037142 A1 Feb. 20, 2003

Related U.S. Application Data

(60) Division 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.** **709/225**; 709/229

(58) **Field of Classification Search** 709/217–225, 709/229; 713/201

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846 A 6/1990 Humphrey et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE 199 24 575 12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Aug. 23, 2002), International Application PCT/US01/13260.

(Continued)

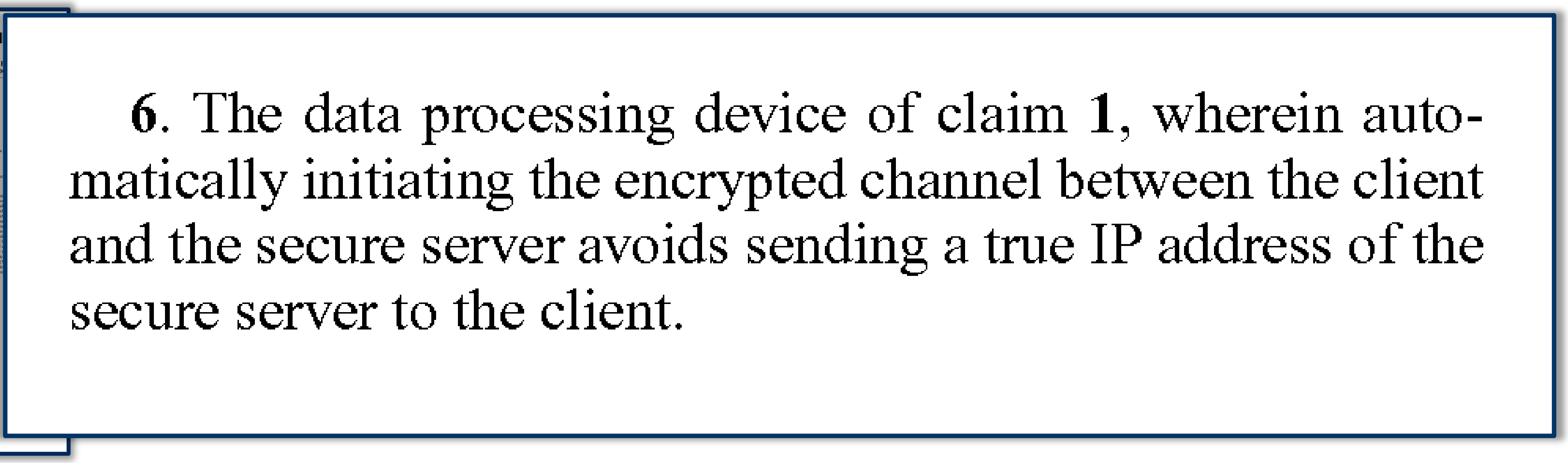
Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—McDermott Will & Emer

(57) **ABSTRACT**

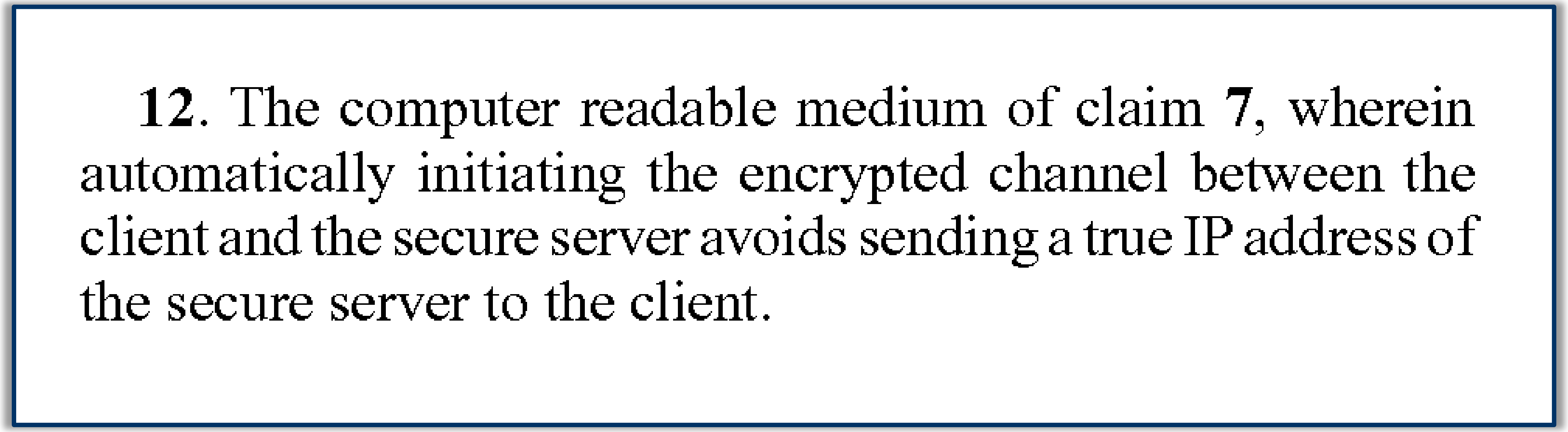
A plurality of computer nodes communicate using seemin random Internet Protocol source and destination address Data packets matching criteria defined by a moving wind of valid addresses are accepted for further processing, wh those that do not meet the criteria are quickly reject Improvements to the basic design include (1) a load balan that distributes packets across different transmission pa according to transmission path quality; (2) a DNS pro server that transparently creates a virtual private network response to a domain name inquiry; (3) a large-to-small l bandwidth management feature that prevents denial-of-s vice attacks at system chokepoints; (4) a traffic limiter t regulates incoming packets by limiting the rate at whic transmitter can be synchronized with a receiver; and (5 signaling synchronizer that allows a large number of node communicate with a central node by partitioning the comm nication function between two separate entities.

16 Claims, 35 Drawing Sheets

100
ORIGINATING TERMINAL
40
IP PACKET
107
22
IP ROUTER
31
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
28
IP ROUTER
29
IP ROUTER
25
IP ROUTER
INTERNET
32
IP ROUTER
27
26
IP ROUTER
DESTINATION TERMINAL



6. The data processing device of claim **1**, wherein automatically initiating the encrypted channel between the client and the secure server avoids sending a true IP address of the secure server to the client.



12. The computer readable medium of claim **7**, wherein automatically initiating the encrypted channel between the client and the secure server avoids sending a true IP address of the secure server to the client.