IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Larson *et al.*
U.S. Patent No.: 7,418,504 Attorney Docket No.: 38868-0005IP2
Issue Date: August 26, 2008
Appl. Serial No.: 10/714,849
Filing Date: November 18, 2003
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

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. 7,418,504, 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 Communications Department, where I worked to develop and deploy an integrated broadband network. From 1992 to 1997, I was the manager of Broadband Networking within IBM's Security and Networking Systems Department, where I led a group of researchers in the area of design, architecture, and analysis of broadband networks. One of the projects on which I worked, for example, led to U.S. Patent No. 5,673,318, which regards "[a]

method and system for providing data authentication, within a data communication environment, in a manner which is simple, fast, and provably secure," and of which I am a named inventor. *See* U.S. Patent No. 5,673,318, abstract. From 1997 to 1998, I was the manager of Network Control and Services within IBM's Security and Networking Systems Department, where I led a department responsible for networking and distributed applications, including topics such as advance reservations, policy support, including for Resource Reservation Protocol (RSVP), quality of service (QoS) routing, and security, and integrated switch and scheduling designs.

4. I have been a professor of engineering for the past fifteen years. As such, but prior to becoming the chair of the Computer Science & Engineering department at Washington University in St. Louis, I was the Alfred Fitler Moore Professor of Telecommunications Networks (an honorary chair) in the Department of Electrical and Systems Engineering at the University of Pennsylvania. As a professor of engineering, I have taught many courses in networking, including Advanced Networking Protocols (TCOM 502), which addressed, among other things, virtual private networks.

5. I have authored over fifty journal publications, including "On the Feasibility and Efficacy of Protection Routing in IP Networks," which was honored as the IEEE INFOCOM 2010 Best Paper Award. I have been named a Fellow by both the IEEE and ACM, and, from 2009 to 2012, I was the Editor-in-Chief of the IEEE/ACM Transactions on Networking. Furthermore, I am a named inventor on over thirty issued U.S. patents.

6. I am familiar with the content of U.S. Patent No. 7,418,504 (the "'504 patent"). In addition, I have considered the various documents referenced in my declaration as well as additional background materials. I have also reviewed certain sections of the prosecution history of the '504 patent, the prosecution history of reexamination control numbers 95/001,788 and

95/001,851; and the claim construction orders from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:07CV80 (E.D. Tex.) and *VirnetX Inc. v. Cisco Systems, Inc. et al.*, Docket No. 6:10cv417 (E.D. Tex.).

7. Counsel has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '504 patent at the time of the invention, and I have done so during my review of these materials. I believe one of ordinary skill as of February 15, 2000 (the priority date of the '504 patent) would have a Master's degree in computer science or computer engineering, or in a related field such as electrical engineering, as well as about two years of experience in computer networking and in some aspect of security with respect to computer networks. I base this on my own personal experience, including my knowledge of colleagues and others at the time.

8. I have no financial interest in either party or in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

9. My opinions, as explained below, are based on my education, experience, and background in the fields discussed above.

10. This declaration is organized as follows:

I. Brief Overview of the '504 Patent

II. Terminology

III. Aventail and Combinations Involving Aventail

IV. Publication and Authenticity for Requests for Comments (RFCs)

V. Conclusion

I. Brief Overview of the '504 Patent

11. A section of the '504 patent's specification titled "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks" describes "the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.," with reference to FIG. 26. Ex. 1001, 39:4-6. Referring to FIG. 26 below, 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." Ex. 1001, 39:63-67. "A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610." Ex. 1001, 39:67 to 40:2. "A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site [2604]." Ex. 1001, 40:2-4. "An 'unsecure' target site 2611 is also accessible via conventional IP protocols." Ex. 1001, 40:4-5.

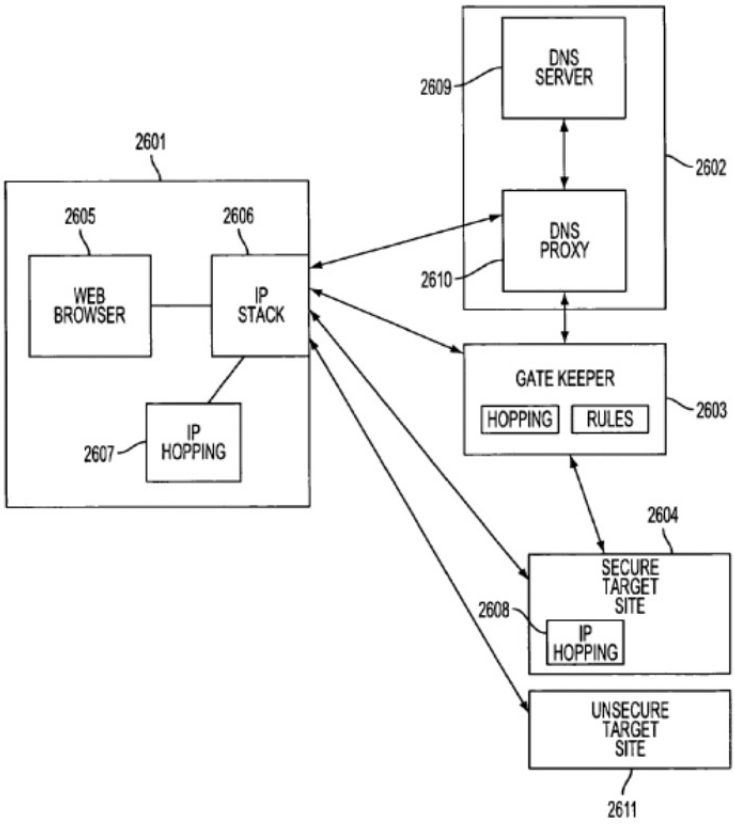

FIG. 26

12. As described by the '504 patent:

DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.