

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Larson *et al.*
U.S. Patent No.: 7,188,180 Attorney Docket No.: 38868-0002IP1
Issue Date: Mar. 6, 2007
Appl. Serial No.: 10/702,486
Filing Date: Nov. 7, 2003
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

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. 7,188,180, 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 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. 7,188,180 (the “180 patent”). Additionally, I have reviewed the following: U.S. Patent No. 6,557,037 to Provino (“Provino”); Alvaro Guillen *et al.*, 1993 International Conference on Network Protocols, *An Architecture for Virtual Circuit/QoS Routing* (Oct. 1993) (“Guillen”); Dave Kosiur, “Building and Managing

Virtual Private Networks” (1998) (“Kosiur”); E. Gavron, RFC 1535, *A Security Problem and Proposed Correction With Widely Deployed DNS Software* (Oct. 1993); RFC 791, *Internet Protocol* (Sep. 1981). I have also reviewed certain sections of the prosecution history of the ‘180 patent, the prosecution histories of reexamination control numbers 95/001,270 and 95/001,792; 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 ‘180 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 April 26, 2000 (the priority date of the ‘180 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 ‘180 Patent (page 4)
- II. Terminology (page 7)
- III. Provino and Combinations Based on Provino (page 11)

IV. Conclusion (page 24)

I. Brief Overview of the '180 Patent

11. The '180 patent is directed to a "method for establishing [a] secure communication link between computers of [a] virtual private network." Ex. 1001, Title. The '180 patent includes 41 claims, of which claims 1, 17, and 33 are independent.

12. A section of the '180 patent's specification titled "F. One-Click Secure On-Line Communications and Secure Domain Name Service" describes "a technique for establishing a secure communication link between a first computer and a second computer over a computer network," with reference to FIGS. 33-35. Ex. 1001, 49:57-59. Referring to Annotation A of FIG. 33 below, a computer 3301 establishes a VPN communication link with a server computer 3320, or a secure edge router for the server computer 3320. See Ex. 1001, 51:16-18, 52:30-33.

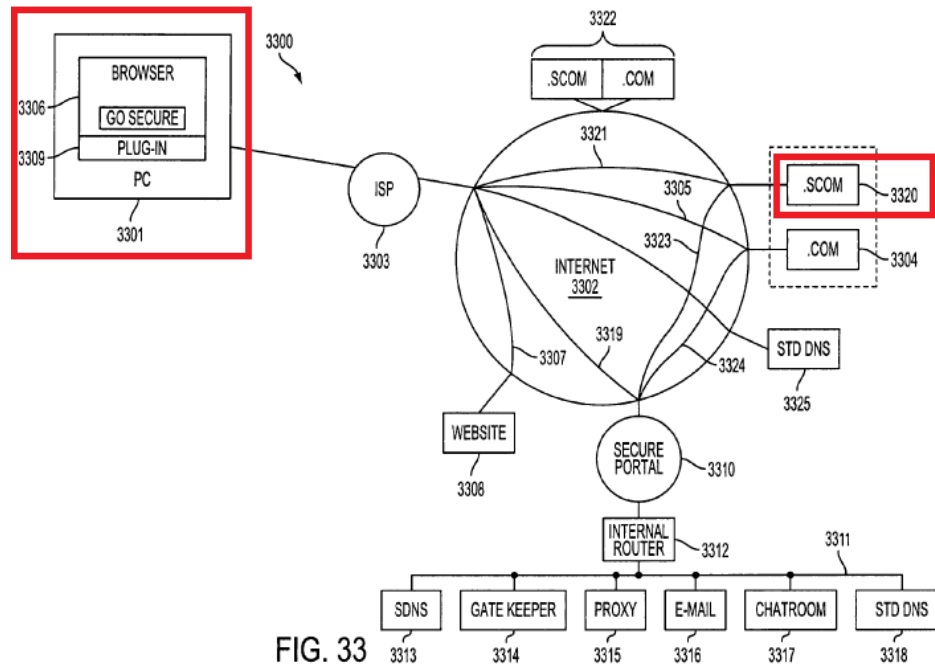


FIG. 33

Annotation A

13. The server computer 3320 is associated with a secure top-level domain name. See Ex. 1001, 51: 21-22. Domain names are a type of human-readable name/address for resources

on a network, such as the Internet. *See* RFC 1535, p. 1 (1993) (“Current Domain Name Server clients are designed to ease the burden of remembering IP dotted quad addresses. As such they translate human-readable names into addresses and other resource records.”). Domain names are resolved by name servers into numerical addresses that are utilized for packet forwarding over networks. *See id.*; *see also* RFC 791, pp. 2, 5-6 (1981). As such, domain names may be maintained in the human-readable form, which is easier for a human operator to utilize than the numerical addresses relied upon by the networks for forwarding packets. Ex. 1003, 1:49-56.

14. With respect to the term “secure top-level domain name,” the ‘180 patent notes that “[b]ecause the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown.” Ex. 1001, 51:29-32. Thus, in the context of the ‘180 patent, a secure top-level domain name is differentiated from a standard domain name in that a secure top-level domain name cannot be resolved by a standard domain name service.

15. In order to resolve the secure top-level domain name of the server computer 3320, the computer 3301 sends a query to a secure domain name service (SDNS) 3313, as illustrated in the following Annotation B of FIG. 33. *See* Ex. 1001, 51:46-50. This query to the SDNS 3313 can either be sent “in the clear” or can use a VPN communication link. *See* Ex. 1001, 52:41-43. With respect to the term “secure domain name service,” the ‘180 patent indicates that “SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses.” Ex. 1001, 52:4-5. In other words, the SDNS 3313 differs from a standard name service in that it is configured to resolve secure domain names.

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.