Attorney Docket No. 077580-0089

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmund Munger, et al.	)	
	)	
U.S. Patent No.: 6,502,135	)	
Filed: February 15, 2000	)	**Examiner:**
Issued: December 31, 2002	)	**Andrew L. Nalven**
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,269	)	
Filed: December 8, 2009	)	

Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132

Pursuant to 37 C.F.R. § 1.132, I declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

Background

1. I have over 15 years of experience with operating systems and distributed systems. More specifically, my experience includes remote access, computer networking, and computer security. Examples of my experience are evidenced by my publication of papers in top-tier networking and security conferences, service on programming committees for networking and security conferences, awards for research work, and receipt of research grants in the field of networking and security. My qualifications, including a description of all of this information, may be found in my curriculum vitae, which is attached hereto as Exhibit A.

2. I earned a Bachelor of Science degree from the Massachusetts Institute of Technology in Electrical Engineering in1989. I earned a Masters of Science degree from Stanford University in Electrical Engineering in 1990. I also received my Ph.D. in Electrical Engineering from Stanford University in 1999.

EXHIBIT A-3

3. I joined Columbia University as a faculty member in 1999, where I am now a tenured Associate Professor in the Department of Computer Science. I am also currently the director of the Network Computer Laboratory at Columbia University.

4. My research interests include mobile computing, operating sstems, distributed systems, thin-client computing, web and multimedia systems, and performance evaluation. I have supervised a number of Ph.D. students who worked on and completed dissertations in the area of networking and security. I also teach courses in advanced operating systems and mobile computing, both of which involve computer networking and security.

5. I have also served as an expert in various litigations in the fields of computer networking and security, which include virtual private networking.

Resources I have Consulted

6. I have been retained by the Patent Owner, VirnetX, Inc., to offer my opinion of the patentability of claims 1, 3, 4, 6-10, and 12 of U.S. Patent Number 6,502,135 ("the '135 Patent") in view of the Office Action dated January 15, 2010 ("the Office Action") received by the Patent Owner in the reexamination of the '135 Patent.

7. In preparing this declaration, I have reviewed the '135 Patent, including the claims. I have also reviewed the outstanding Office Action. I have also reviewed the Request for *Inter Partes* Reexamination of Patent ("the Request") to the extent it is adopted by the Office Action. I have also reviewed Appendix A to the Request ("Appendix A") to the extent that it is adopted in the Office Action. Lastly, I have reviewed Aventail Connect v3.1/v2.6 Administrator's Guide ("Aventail"), the reference upon which the rejection in the Office Action is based.

8. A detailed explanation of the basis for my opinions is set forth in the remainder of this declaration.

Detailed Basis for My Opinion

I provide here a brief description of the system disclosed in Aventail.

9. As I stated above, I have read the '135 Patent, including the claims, and understand independent claim 1 to recite "[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."

10. Similarly, I understand independent claim 10 to recite "[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."

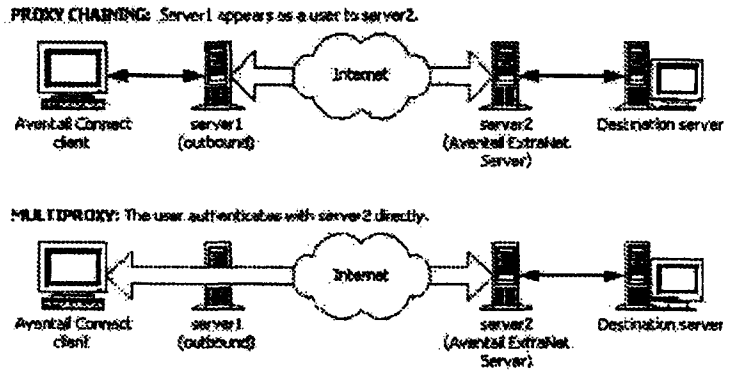
11. After reviewing the Aventail reference, I understand Aventail to disclose a system for transmitting data between two computers using the SOCKS protocol. The system according to Aventail routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Upon receipt of the network traffic, the SOCKS server then transmits the network traffic to the Internet or external network. Aventail's disclosure is limited to connections created at the socket layer of the network architecture.

12. I note that pages 9-12 of Aventail discuss the basics of the operation of Aventail Connect, the software necessary to implement the system disclosed in Aventail. According to page 9 of Aventail, a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. Accordingly, Aventail Connect is able to intercept all connection requests from the user, and determines whether each request matches local, preset criteria for redirection to a SOCKS server.

13. According to page 12 of Aventail, if redirection is appropriate, then Aventail Connect creates a false DNS entry to return to the requesting application. Aventail discloses that Aventail Connect then forwards the destination hostname identified in the DNS request to the extranet SOCK server over a SOCKS connection.

14. Although Aventail is generally silent on the operation of the SOCKS server, I understand from page 12 that the SOCKS server performs the hostname resolution. Once the hostname is resolved, the user can transmit data over a SOCKS connection to the SOCKS server. The SOCKS server, then, separately relays that transmitted data to the target.

15. Page 12 of the Request also cites to the "Proxy Chaining" and "MultiProxy" modes disclosed in Aventail at pages 68-73. I have reproduced below a figure taken from page 72 of Aventail depicting these two modes.



16. In the "Proxy Chaining" mode, Aventail indicates that a user can communicate with a target via a number of proxies such that each proxy server acts as a client to the next downstream proxy server. As shown above, in this mode, the user does not communicate directly with the proxy servers other than the one immediately downstream from it.

17. In the "MultiProxy" mode, Aventail indicates that the user, via Aventail Connect, authenticates with each successive proxy server directly.

18. Regardless of whether one of these modes is enabled, as shown in the figure, an external SOCKS server is necessary and the operation of Aventail Connect, for the purposes of my opinion, does not materially differ based on whether one of these modes is enabled.

Aventail has not been shown to disclose a virtual private network according to claim 1.

19. Aventail has not been shown to disclose the VPN claimed in claim 1 of the '135 Patent for at least three reasons.

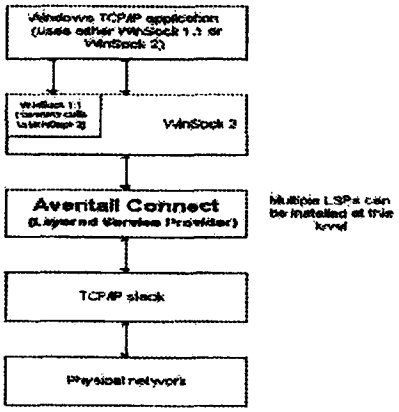
20. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network. Aventail discloses establishing a point-to-point SOCKS connection between a client

computer and a SOCKS server. According to Aventail, the SOCKS server then relays data received to the intended target. Aventail does not disclose a VPN, where data can be addressed to one or more different computers across the network, regardless of the location of the computer.

21. For example, suppose two computers, A and B, reside on a public network. Further, suppose two computers, X and Y, reside on a private network. If A establishes a VPN connection with X and Y's network to address data to X, and B separately establishes a VPN connection with X and Y's network to address data to Y, then A would nevertheless be able to address data to B, X, and Y without additional set up. This is true because A, B, X, and Y would all be a part of the same VPN.

22. In contrast, suppose, according to Aventail, which only discloses communications at the socket layer, A establishes a SOCKS connection with a SOCKS server for relaying data to X, and B separately establishes a SOCKS connection with the SOCKS server for relaying data to Y. In this situation, not only would A be unable to address data to Y without establishing a separate SOCKS connection (the alleged VPN according to the Office Action), but A would be unable to address data to B over the secure connection. This is one example of how the cited portions of Aventail fail to disclose a VPN.

23. Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users attempting to transmit data that is sensitive to network information. As I stated above, Aventail discloses that Aventail Connect operates between the WinSock and TCP/IP layers. The figure I have reproduced below from page 9 of Aventail depicts this operation.



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.