

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

|   |   |                         |
|---|---|-------------------------|
| In re <i>Inter Partes</i> Reexamination of: | ) |                         |
|   | ) |                         |
| Victor Larson et al.                        | ) | Control No.: 95/001,788 |
|   | ) |                         |
| U. S. Patent No. 7,418,504                  | ) | Group Art Unit: 3992    |
|   | ) |                         |
| Issued: August 26, 2008                     | ) | Examiner: Roland Foster |
|   | ) |                         |
| For: AGILE NETWORK PROTOCOL FOR SECURE      | ) | Confirmation No. 5823   |
| COMMUNICATIONS USING SECURE                 | ) |                         |
| DOMAIN NAMES                                | ) |                         |

Mail Stop *Inter Partes* Reexam  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**DECLARATION OF DR. ROBERT DUNHAM SHORT III**

I, Robert Dunham Short III, declare as follows:

1. I have been the Chief Technology Officer of VirnetX Inc. ("VirnetX") since June 2010 and the Chief Scientist for VirnetX since May 2006. Prior to joining VirnetX, from 1994 to April 2006, I held various positions including Assistant Vice President and Division Manager at Science Applications International Corporation ("SAIC"). Prior to SAIC, I worked at ARCO Power Technologies Inc., Sperry Corporate Technology Center, and Sperry Research Center. I have a Ph.D. in Electrical Engineering from Purdue University as well as a M.S. in Mathematics and a B.S. in Electrical Engineering from Virginia Tech.

2. I am one of the named inventors of U.S. Patent No. 7,418,504 ("the '504 patent"), which I understand is the subject of the above-identified reexamination proceeding. I am familiar with the '504 patent, including its claims.

3. Prior to and at the time of the inventions claimed in the '504 patent, there was a significant and increasing concern with the security of computer network communication. The widespread connectivity between computers that was enabled by the swift increase in network access in homes and businesses also led to many security breaches as well as concerns regarding the safety of confidential information sent over computer networks. This problem received significant attention from the research and development community. Practical experience showed that there was a need for a system that could be easily and correctly used to enable secure communications, because a system that made it difficult for an end-user to enable secure communications would likely lead to a

lack of use or incorrect use. The inventions disclosed and claimed in the '504 patent and other patents in this family met this need. For instance, the inventions disclosed and claimed in the '504 patent include a domain name service for establishing secure communication links. As an example, independent claim 1 recites “[a] system for providing a domain name service for establishing a secure communication link, the system comprising[] a domain name service system configured . . . to comprise an indication that the domain name service system supports establishing a secure communication link.” ('504 patent 55:49-56.) Dependent claim 8 recites that the domain name service system is connectable to a virtual private network (VPN) through the communication network and dependent claim 9 recites that the virtual private network is one of a plurality of secure communication links in a hierarchy of secure communication links. ('504 patent 56:5-10.) Further, dependent claim 16 recites that the “domain name service system is configured to support establishing a secure communication link between [a] first location and [a] second location.” ('504 patent 56:40-43.) As another example, claim 27 recites that the domain name service system is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location. ('504 patent 57:13-16.) The inventions combine both ease-of-use and security aspects without sacrificing one or the other.

4. As one example of the manifestation of the long-felt need, the Defense Advanced Research Projects Agency (“DARPA”) funded various research programs to further the science and technology of information assurance and survivability. DARPA programs, such as the “Information Assurance” and “Dynamic Coalitions” programs, were focused on the need to provide easy-to-enable secure communications. These projects received significant funding to be spent developing technologies that could solve this need. For example, one such project entitled “Next Generation Internet” received funding in fiscal year 1998 of approximately \$39.3 million, in fiscal year 1999 of approximately \$49.5 million, and in fiscal year 2000 of approximately \$40 million. (Ex. B-1 at VNET00219302, 319-321.) Another program funded by DARPA, “Dynamic Coalitions,” was created to address the ability of the Department of Defense to quickly and easily enable secure communications over the Internet. (See, e.g., Ex. B-2 at VNET00219244, 284, 298-299, 593, 625.)

5. According to DARPA officials at the time, “existing group membership protocols d[id] not support the security needs of multidimensional organizations. The overarching challenge [wa]s creating secure groups rapidly. This [wa]s a significant issue when countries [we]re faced with an operation that require[d] immediate multinational attention.” (Ex. B-3 at 1.) DARPA contracted with some of the most skilled organizations in the area of secured communications in an effort to meet its security needs (e.g., NAI Labs, a division of PGP Security, Network Associates Incorporated, Los

Angeles, and the Microelectronics Center of North Carolina, Research Triangle Park, North Carolina, as well as Johns Hopkins University, Baltimore; Northeastern University, Boston; and Veridian-PSR, Arlington, Virginia). (*Id.* at 1.) In all, more than 15 organizations were researching the various components that made up the programs initiated by the Department of Defense. (*Id.*) However, none of these prestigious institutions came up with a solution, during the relevant time frame, close to what is disclosed and claimed in the '504 patent. (*Id.* at 1-4.) That is, they did not develop a solution that provided a domain name service for establishing a secure communication link.

6. As a second example of the long-felt need for the inventions of the '504 patent, In-Q-Tel, which is a venture capital firm that invests in companies developing cutting edge technology aimed at supporting the United States intelligence community, including the Central Intelligence Agency (CIA), funded the original development of the technology with approximately \$3.4 million. In-Q-Tel's willingness to enter into a relationship with SAIC (the original assignee of the application that led to the '504 patent) for the development of this technology further evidences a long-felt need for technology that made it easy and convenient to enable secure communications.

7. A third example was the extent to which SAIC internally funded the research and development of the technology. When I was employed at SAIC, its business model was to sell hours to the federal government. SAIC was not structured to bring products to the market, which typically requires significant internal investments in research and development. In an average year during the development of the technology that led to the '504 patent, SAIC would spend approximately \$2 million on internal research and development efforts. In the case of the technology claimed in the '504 patent, SAIC invested \$1.7 million, which represents almost the entirety of SAIC's internal research and development budget for one whole year. A technology review committee also approved our team's patent development efforts and costs on an ongoing basis. A third party (Cambridge Strategic Management Group or CSMG) also substantiated the value of the technology. Moreover, a significant percentage of all of SAIC's patent development efforts have focused on this technology. I understand that SAIC spent one-third of its total patent portfolio efforts on our patent portfolio at that time.

8. In fact, as demonstrated in an article written before the claimed inventions of the '504 patent, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. (Ex. B-4 at 1.) In that time period, remote access was "a nightmare for support desks. Staffers never kn[e]w what combination of CPU, modem, operating system and software configuration they [were] going to have to support," and adding the commercially-available VPN software only made matters worse. (*Id.*)

9. This article precisely captured the computer and Internet security industry's attitude toward the tradeoff between the ease of use of a secure system, such as a VPN system, for the average computer user and the security that the VPN system provided. The article recognized that the "ease of installation isn't always a good thing: In many cases, the easier the client is to install, the less secure it is." (*Id.* at 2.) The claimed inventions of the '504 patent, which provide a domain name service for establishing a secure communication link (for example, a VPN communication link), combine both ease of use and security aspects without sacrificing one or the other.

10. Moreover, many others before and around the time of the inventions claimed in the '504 patent have attempted to solve the need of easy-to-use methods of enabling secure communications over the Internet. But, as discussed above, many of these attempts have failed. For example, despite investing enormous amounts of money and enlisting the resources of numerous prestigious institutions and their talented employees, DARPA's projects still fell far short of the claimed inventions of the '504 patent. (*See* ¶¶ 4-5, *supra.*)

11. Additionally, as discussed above, no one had yet achieved the results of the claimed inventions of the '504 patent in that time period, because remote access was "a nightmare" for support desks to handle, and adding the commercially-available VPN software was even more difficult. In fact, at this time, the security industry generally viewed ease of use and VPN security as mutually exclusive. (*See* ¶¶ 8-9, *supra.*) By providing a domain name service for establishing a secure communication link, the inventions of the '504 patent provided a system for easily establishing secure communication links without sacrificing security, thereby succeeding where others failed.

12. The claimed inventions of the '504 patent have been commercially successful, for example, through the licensing revenues they have generated for VirnetX. In July 2002, SafeNet, a leading provider of Internet security technology that is the de facto standard in the VPN industry, entered into a portfolio license with SAIC to incorporate features into SafeNet's underlying VPNs. SafeNet licensed the patents because of features disclosed and claimed in the patents, including those in the '504 patent. Microsoft has also entered into a similar license that includes the '504 patent. Microsoft entered into its license with VirnetX after it was found to have infringed two other VirnetX patents in the same family, resulting in a damages award of over one hundred million dollars, leading ultimately to a license agreement of two hundred million dollars.

13. The claimed inventions of the '504 patent were also contrary to the accepted wisdom at the time of the inventions. For example, there was a general understanding that reliable security could only be achieved through difficult-to-provision VPNs and easy-to-set-up connections could not be secure. This belief was reinforced by the IT offices of many large companies and institutions,

whose livelihood depended on the need for highly-trained specialists to arrange secure network connections.

14. The industry had long accepted as a fact that secure systems, such as VPN systems, would be difficult to set up, and the secure communication modes could not be easily and conveniently enabled. In a 1999 article entitled "CEOs Chew the VPN Fat" that predicted what the future held for the start-up companies that developed VPNs, the wish list did not even address the type of solutions provided by the '504 patent, such as a domain name service for establishing secure communication links. (Ex. B-5 at 1-2.)

15. The technology of the '504 patent was also met with skepticism by those skilled in the art who learned of our inventions. Sami Saydjari, a program manager for DARPA, informed Edmund Munger, a co-inventor of the '504 patent, that our technology would never be adopted. Moreover, the IT offices of many large companies and institutions expressed skepticism that secure connections could ever be enabled easily by regular computer users.

16. Several events also demonstrate praise for the inventions in the '504 patent by those in the field. As discussed above, SAIC invested a disproportionately large percentage of its internal resources in the technology. SafeNet and Microsoft have both licensed the technology of the '504 patent. A study done by CSMG also praised the inventions. Jim Rutt at Network Solutions, which was acquired by Verisign, praised and expressed significant interest in the technology and would have invested but for a change in circumstances at his company.

17. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the '504 patent.

Dated: March 29, 2012

By:           /Robert Dunham Short III/          

Robert Dunham Short III