IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* 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 COMMUNICATIONS USING SECURE DOMAIN NAMES	)	Confirmation No.: 5823

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

Declaration of Angelos D. Keromytis, Ph.D.

I declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

I, ANGELOS D. KEROMYTIS, declare as follows:

1. I have been retained by VirnetX Inc. ("VirnetX") for the above-referenced reexamination proceeding. I understand that this reexamination involves U.S. Patent No. 7,418,504 ("the '504 patent"). I further understand that the '504 patent is assigned to VirnetX and that it is part of a family of patents ("Munger patent family") that stems from U.S. provisional application nos. 60/106,261 ("the '261 application"), filed on October 30, 1998, and 60/137,704 ("the '704 application"), filed on June 7, 1999. I understand that the '504 patent is a continuation of U.S. application no. 09/558,210 ("the '210 application"), filed April 26, 2000 (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent No. 6,502,135, "the '135 patent"). I also understand that the '135 patent is a continuation-in-part of U.S. application no. 09/429,643 (now U.S. Patent No. 7,010,604), which claims priority to the '261 and '704 applications.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

I. RESOURCES I HAVE CONSULTED

2. I have reviewed the '504 patent, including claims 1-60. I have also reviewed a Request for *Inter Partes* Reexamination of the '504 patent filed by Apple Inc. with the U.S. Patent and Trademark Office on October 18, 2011 ("Request" or "Req."), as well as its accompanying exhibits.[1] Additionally, I have reviewed an Order Granting Request for *Inter Partes* Reexamination of the '504 patent ("the Order") and an Office Action ("the Office Action"), both mailed on December 29, 2011.[2]

3. I have also studied the following documents cited in and included with the Request and/or Office Action: E. Solana et al., "Flexible Internet Secure Transactions Based on Collaborative Domains," Lecture Notes in Computer Science, vol. 1361, at 37-51 (1997) ("*Solana*"); U.S. Patent No. 6,557,037 to Provino ("*Provino*"); U.S. Patent No. 6,496,867 to Beser et al. ("*Beser*"); R. Atkinson, IETF RFC 2230, "Key Exchange Delegation Record for the DNS," November 1997 ("RFC 2230"); D. Eastlake et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)," March 1999 ("RFC 2538"); S. Kent et al., IETF RFC 2401, "Security Architecture for the Internet Protocol," November 1998 ("RFC 2401"); D. Eastlake et al., IETF RFC 2065, "Domain Name System Security Extensions," January 1997 ("RFC 2065"); J. Postel et al., IETF RFC 920, "Domain Requirements," October 1984 ("RFC 920"); E. Guttman et al., IETF RFC 2504, "Users' Security Handbook," February 1999 ("RFC 2504"); M. Reed et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA (December 9-13) ("*Reed*"); Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK, May 1996 ("Goldschlag"); P. Mockapetris, IETF RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC 1035"); R. Braden, IETF RFC 1123, "Requirements for Internet Hosts – Applications and Support," October 1989 ("RFC 1123"); R. Atkinson, IETF RFC 1825, "Security Architecture for the Internet Protocol," August 1995 ("RFC 1825"); R. Housley et al., IETF RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and

---

[1] I refer to the Request for *Inter Partes* Reexamination as "the Request" and, correspondingly, I will refer to Apple Inc. as "the Requester."

[2] The Office Action incorporates nearly all of the Request by reference. For that reason, when I sometimes refer to "the Request," I am also referring to the Office Action.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

CRL Profile," January 1999 ("RFC 2459"); and P. Mockapetris, IETF RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC 1034").[3]

4. I am familiar with the level of ordinary skill in the art with respect to the inventions of the '504 patent as of February 15, 2000, when the application for the parent '135 patent was filed. Specifically, based on my review of the technology, the educational level of active workers in the field, and drawing on my own experience, I believe a person of ordinary skill in art at that time would have had a master's degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security.

5. I have been asked to consider how one of ordinary skill in the art would have understood the references mentioned above. My findings are set forth below.

II. QUALIFICATIONS

6. I have a great deal of experience and familiarity with computer and network security, and have been working in this field since 1993.

7. I am currently an Associate Professor of Computer Science at Columbia University, as well as Director of the University's Network Security Laboratory. I joined Columbia in 2001 as an Assistant Professor, after receiving my M.Sc. and Ph.D. degrees in Computer Science, both from the University of Pennsylvania. My Ph.D. dissertation work was on the topic of secure access control for distributed systems and, in particular, on the management of trust in distributed computer networks.

8. I received my B.Sc. in Computer Science from the University of Crete, in Greece, in 1996. During my undergraduate studies, I worked as system administrator in the Computing Center at the University of Crete. Following that, I worked as network engineer at the first commercial Internet Service Provider ("ISP") in Greece, FORTHnet SA, where I was exposed to many network security issues.

9. I have actively participated in the Internet Engineering Task Force ("IETF"), a standards-setting body for the Internet, since 1995. In the late 1990s and early 2000s, my work with the IETF was primarily within the Internet Protocol Security ("IPsec") Working Group. In addition

[3] Although I listed dates in these citations, I am not testifying to whether any of these references were actually publicly distributed on the date listed.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

to contributing to the specification of the IPsec standards, I wrote the first implementation of the Photuris key management protocol (now RFC 2522). I also contributed to the first open-source implementation of the IKSAMP/IKE key management protocol for the open-source BSD operating system (now RFC 2409), and developed the first such implementation for the Linux operating system. My Linux implementation, named Pluto, was adopted by the National Institute of Standards and Technology ("NIST") in 1999. In addition, my implementation of IPsec for the open-source BSD operating system is currently used by many companies and governments around the world, and serves as the basis for several commercial products that employ cryptographic communications. In 1999, I architected and implemented the first open-source framework for supporting hardware cryptographic accelerators. This framework is used in the open-source OpenBSD, NetBSD, FreeBSD, and Linux operating systems. My work in implementing firewalls and other cryptographic and network protocols has resulted in commercial systems and publications in refereed technical conferences and academic journals. I served as Working Group Secretary for the IETF IPsec Working Group (2003-2005) and as Security Area Advisor to the IETF at large (2003-2008).

10. In my current position at Columbia University, I work with a large group of graduate and postgraduate students in the area of cybersecurity. My past students now work in this field as university professors, as technical researchers for research laboratories, or as engineers for telecommunications companies. I have received federal, state, and corporate sponsorship to conduct cybersecurity research from the Department of Defense, the National Security Agency, the Defense Advanced Research Projects Agency ("DARPA"), the National Science Foundation, the Department of Homeland Security, the Air Force, the Office for Naval Research, the Army Research Office, the Department of the Interior, the National Reconnaissance Office, New York State, Google, Intel, Cisco, and others. In my ten years as a professor, I have received over 36 million dollars to support my research in cybersecurity. I also regularly teach courses on cybersecurity, in addition to more general courses in computer science.

11. I have published over 200 technical papers in refereed journals, conferences, and workshops, all of which are directed to various areas of cybersecurity. I have also authored a book, coauthored another book, and contributed chapters for many other books that relate to cybersecurity. Between 1999 and 2010, I have drafted or codrafted eight standards documents that were published as Request for Comments ("RFCs"). Several of these RFCs are directly related to IP security. For example, RFC 6042 relates to transport layer security; RFC 5708, RFC 2792, and RFC 2704 relate to key signature and encoding for trust management; and RFC 3586 relates to IP security policy

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

requirements. Additionally, I am a coinventor on twelve issued U.S. patents, and have several other applications pending. Most of these patents and pending applications are related to network and systems security.

12. I have chaired several international technical conferences and workshops in cybersecurity, including, for example, the International Conference on Financial Cryptography and Data Security (FC), ACM Computer and Communication Security (CCS), and the New Security Paradigms Workshop (NSPW). I have also served in over eighty technical program committees for such events. From 2004-2010, I served as Associate Editor for the premier technical journal on cybersecurity—the ACM Transactions on Information and Systems Security (TISSEC). Additionally, I have served on several advisory workshops to the United States Government on cybersecurity, including, among others, the Office of the Director of National Intelligence (ODNI)/National Security Agency (NSA) Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E) (2011), the Office of Naval Research (ONR) Workshop on Host Computer Security (2010), the Intelligence Community Technical Exchange on Moving Target (2010), Lockheed Martin Future Security Threats Workshop (2009), and the ARO/FSTC Workshop on Insider Attack and Cyber Security.

13. In addition to this work, I have cofounded two companies in cybersecurity. One company, StackSafe Inc. (formerly Revive Systems Inc.), was a provider of a virtualized preproduction staging environment that includes automated testing, analysis, and reporting for IT operations teams. I was with this company from its founding in 2005 until 2009. The second company, Allure Security Technologies (founded in 2010), develops deception-based solutions for detecting and mitigating the malicious cyber-insider threat, commercializing technology developed at Columbia through DHS and DARPA grants and a DARPA SBIR contract.

14. My curriculum vitae, which is appended to this declaration, details my background and technical qualifications. Although I am being compensated at my standard rate of $500/hour for my work on this declaration, the compensation in no way affects the statements in this declaration.

III. BACKGROUND OF THE '504 PATENT

15. Before turning to a discussion of the references relied on in the Request and the Office Action, I summarize my understanding of certain embodiments disclosed in the '504 patent. Generally speaking, the '504 patent discloses, among other things, systems and methods for providing a domain name service ("DNS") for establishing a secure communication link.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.