UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

In re
Inter Partes Review of
U.S. Patent No.: 6,502,135
Inventors: Munger *et al.*
Issue Date: Dec. 31, 2002

Trial Number: IPR2013-00375

Title: Agile Network Protocol for Secure Communications With Assured System Availability

Attorney Docket No. 3959/5001

Attn: Mail Stop PATENT BOARD
Patent Trial and Appeal Board
United States Patent and Trademark Office
PO Box 1450
Alexandria, Virginia 22313–1450

Declaration of Russell Housley Regarding U.S. Patent No. 6,502,135

I, Russell Housley, do hereby declare and state, 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.

Dated: 22 June 2013

Russell Housley

I, Russell Housley, declare as follows:

I. INTRODUCTION

A. Engagement

1. I have been retained by counsel for New Bay Capital, LLC as an expert witness in the above-captioned proceeding. I submit this declaration in support of the Petition for Inter Partes Review (hereinafter "the Petition") of claims 1, 3, 7 and 8 of United States Patent No. 6,502,135 (hereinafter "the '135 Patent" – Exhibit 1001), filed in the United States Patent and Trademark Office on behalf of New Bay Capital, LLC.

B. Background and Qualifications

2. I am the founder and owner of Vigil Security, LLC, which I founded in 2002 to help customers design and implement diligently watchful security solutions. I provide consulting on security protocols, security architectures, and Public Key Infrastructure (PKI). Over the last ten years, I have performed security and vulnerability analyses of various communications architectures and security policies based on known threats and proposed certification criteria.

3. Since March 2013, I have served as the chair of the Internet Activities Board (IAB), which is a voting member of the IAB as well as a non-voting

member of the Internet Engineering Steering Group (IESG), a voting member of the IETF Administrative Oversight Committee (IAOC), and a Trustee for the IETF Trust. Since May 2013, I have served as a member of the Internet Research Steering Group (IRSG).

4. From March 2007 to March 2013, I served as the chair of the Internet Engineering Task Force (IETF). I managed the open and transparent technical standards process for the Internet.

5. From March 2003 to March 2007, I served as the IETF Security Area Director, making me a member of the IESG. As such, I provided leadership to many working groups that were developing security standards for the Internet, including the Public Key Infrastructure using X.509 (PKIX), IP Security (IPsec), Transport Layer Security (TLS), Secure MIME (S/MIME), Domain Keys Identified Mail (DKIM), Long-Term Archive and Notary Services (LTANS), and Multicast Security (MSEC) working groups.

6. Prior to accepting the Area Director position, I chaired the IETF Secure MIME (S/MIME) Working Group, and I contributed to several cornerstone Internet PKI standards (including RFC 5280). In November 2004, I was recognized by the IEEE 802.11 working group for my contributions to IEEE 802.11i-2004, which fixes the severe security shortcoming of the Wired Equivalent Privacy (WEP). I provided major contributions to several security protocols, including the

Cryptographic Message Syntax (CMS), SDNS Security Protocol 4 (SP4), SDNS Message Security Protocol (MSP), IEEE 802.10b Secure Data Exchange (SDE) Protocol, and IEEE 802.10c Key Management Protocol.

7. I have worked in the computer and network security field since 1982. Before starting Vigil Security, I worked at the Air Force Data Services Center (AFDSC), Xerox Special Information Systems (XSIS), SPYRUS, and RSA Laboratories. My security research and standards interests include security protocols, certificate management, cryptographic key distribution, and high assurance design and development practices. I have been active in many security standards organizations, and my recent focus has been on the Internet Engineering Task Force (IETF).

8. I have served as the Chair of CertiPath Policy Management Authority, where I assisted with the transition from SHA-1 to SHA-256. I also provided technical and policy advice to the WiMAX Forum Policy Authority for the PKI that is used to authenticate WiMAX Devices and the separate PKI that is used to authenticate the AAA servers within a WiMAX network.

9. I am a Consultant to the U.S. Government. I helped with Crypto Modernization activities, especially in the areas of secure firmware loading, trust anchor management, public key infrastructure, and key management infrastructure.

10. I am a member of the Advisory Board for the Georgetown Center for Secure Communications (GCSC) at Georgetown University, the Security and Software Engineering Research Center (S2ERC) at Georgetown University, and the Center for Information Assurance at the University of Dallas, Graduate School of Management. I am a technical advisor to Penango.

11. I received a Bachelor of Science in computer science from Virginia Tech in 1982, and I received a Master of Science degree in computer science from George Mason University in 1992.

12. I am the co-author of two books: *Implementing Email and Security Tokens: Current Standards, Tools, and Practices*, published by John Wiley & Sons in 2008, and *Planning for PKI – Best Practices Guide for Deploying Public Key Infrastructure*, published by John Wiley & Sons in 2001.

13. I am the inventor of five U.S. Patents:

- US Patent 6,003,135: Modular security device
- US Patent 6,088,802: Peripheral device with integrated security functionality
- US Patent 6,904,523: Method and system for enforcing access to a computing resource using a licensing attribute certificate
- US Patent 6,981,149: Secure, easy and/or irreversible customization of cryptographic device
- US Patent 7,356,692: Method and system for enforcing access to a computing resource using a licensing attribute certificate.

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.