IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Asghari-Kamrani, et al.	
U.S. Patent No.:	8,266 ,432	Attorney Docket No.: 36137-0007IP1
Issue Date:	September 11, 2012	
Appl. Serial No.:	12/210,926	
Filing Date:	September 15, 2008	
Title:	CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD	

DECLARATION OF SETH NIELSON

I. Personal Work Experience and Awards

1. My name is Seth Nielson, Adjunct Associate Research Scientist at The Johns Hopkins University. I am also currently a Principal at Harbor Labs, Inc., an independent consulting firm. In addition to the below summary, a copy of my current curriculum vitae more fully setting forth my experience and qualifications is submitted herewith as Appendix A.

2. I have more than 15 years of dual industrial and academic experience in Computer Science. I received a B.S. in Computer Science in 2000 and my M.S. in Computer Science in 2004, both from Brigham Young University in Provo, UT. I received my Ph.D. in Computer Science in 2009 from Rice University in Houston, TX. My doctoral dissertation concerned "Designing Incentives for Peer-to-Peer Systems." I am the recipient of the Brown Fellowship and a Graduate Fellowship from the Rice University Computer Science Department. I was also a John and Eileen Tietze Fellow.

3. During my final undergraduate semester, I worked both as a teaching assistant for the Computer Networking course and as a researcher in the Networked Computing Lab. In these capacities, I assisted students in debugging and designing their TCP/IP protocol stacks, ARP protocol implementations, and RPC projects. I also collaborated in investigating statistical traffic engineering for bandwidth allocation which culminated in a published paper entitled, "Effective Bandwidth for Traffic Engineering."

4. Effective bandwidth relates to the concept of bandwidth reservation for quality of service guarantees. On data connections designed to carry large quantities of data for many users, some users may pay extra to guarantee a certain quality of service. Nevertheless, given enough users, at any given time some percentage of users with guarantees will not be utilizing their full capacity. Effective bandwidth is a statistical model that dictates how many users can be guaranteed service under these conditions.

5. During my graduate work I have also published additional papers related to networking and computer security. In 2005, I published a paper entitled, "A Taxonomy of Rational Attacks." This paper categorized and described the various types of attacks that one might see in a decentralized, peer-to-peer (p2p) network. When there is no centralized authority, users have to cooperate to obtain

service. Rational attacks refers to the economic incentives to not cooperate while still exploiting the system for service.

6. My thesis, "Designing Incentives for Peer-to-Peer Systems" built on this concept. Given a network where participants cannot be forced to cooperate, the operation of said network must induce cooperation by design of the outcomes. In other words, it must be in each participant's best interest to contribute to the cooperative operation. Experiments included simulated extensions to the BitTorrent peer-to-peer protocol for long-term identities and mechanisms for cooperative anonymity. I constructed my own simulator of the BitTorrent protocol, and simulated thousands of hours of operations. For further accuracy and realism, I cooperated with researchers at other universities that provided me with real data traces of BitTorrent users that used long term identifiers such as a login name.

7. From 2001 through 2003, I worked as a software engineer at Metrowerks (formerly Lineo, Inc.). There I gained substantial experience in software architecture, computer networking, and technical project management. In particular, I developed and maintained the GUI for the Embedix SDK, ported the Linx GUI of the Embedix SDK to Windows, created an automated system to forward Linux python scripts to a Windows GUI, and developed a packaging and automated updating system for client software.

8. During the 2004 fall semester of my Ph.D. program at Rice University, I identified a security vulnerability in the Google Desktop Search that could have allowed hackers to compromise users' computers and obtain private information. After contacting Google and assisting them in closing the vulnerability, we published the details of our investigation.

9. Later, in 2005, I completed an internship at Google, where I designed and implemented a solution to privacy loss in Google Web Accelerator. The Google Web Accelerator was designed to increase the speed of browsing the Internet. Once installed on a user's computer, the browser would request all content through a Google Proxy. The proxy performed pre-fetching and extensive caching in order to provide fast and responsive service to the user. At the time of my internship, news reports had identified odd problems in which users of the Accelerator were accessing other individual's private pages. During my internship, I designed and implemented a prototype solution for this issue.

10. From 2005 through 2011, I worked as a Security Analyst and later a Senior Security Analyst for Independent Security Evaluators. There, I developed a parallel-processing based security tool, developed a FIPS-certified encryption library, developed hardware-accelerated encryption algorithms, developed encrypted file-system prototypes, developed an encryption library for an ISE client, performed port-scanning analyses, evaluated security protocols using formal

methods and hand analysis, and evaluated security failures. I also designed and managed the implementation of a secure communication technology that splits trust between multiple SSL Certificate Authorities (CA), so that if one CA is compromised, the communication stream can still be safely authenticated. My work on the secure communications technology project led to the issuance of multiple patents including U.S. 8,745,372 entitled ―Systems and Methods for Securing Data in Motion.

11. In 2011, I began work as a Research Scientist at Harbor Labs. I am now a Principal, specializing in network security, network communications, software architecture, and programming languages. I have analyzed an extensive collection of commercial software, including software related to secure email, cloud-based multimedia delivery, document signing, anti-virus and anti-intrusion, high-performance routing, networking protocol stacks in mobile devices, PBX telecommunications software, VoIP, and peer-to-peer communications. I have also analyzed security considerations for potential technology acquisitions, re-created heuristic signatures for 1995-era viruses, and re-created a 1995-era network for testing virus scanners of that time period in gateway virus scanning. I, and teams under my direction, also review technologies for compliance with various standards such as HIPAA and also for security vulnerabilities.

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.