

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INCORPORATED
Petitioner

v.

LEON STAMBLER
Patent Owner

Case CBM2015-00044
Patent No. 5,793,302

DECLARATION OF SETH NIELSON, PH.D.

I, Seth James Nielson, hereby declare that I have personal knowledge of the following facts and am competent to testify as follows:

1. I summarize my qualifications for forming the opinions set forth in this declaration below. Those qualifications are described in more detail in my *curriculum vitae* attached as **Exhibit A**. In short, I am an expert in the fields of computer security and networking.

2. I am a Principal at Harbor Labs in Baltimore, Maryland and an Adjunct Associate Research Scientist at Johns Hopkins University.

3. 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.

4. 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.”

5. 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.

6. 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.

7. 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.

8. 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 Linux 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.

9. 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.

10. 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.

11. 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.

12. 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 and firewalls, 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.

13. In particular, I have reviewed and analyzed the design and implementation of multiple security-related gateway products. This includes industrial-grade firewalls that employ anti-virus and anti-malware engines for processing network traffic. I have also reviewed other gateway products that provide secure storage to cloud devices.

14. I have also assessed the security and privacy technologies and policies provided by a third-party vendor to the Center for Copyright Infringement (CCI). CCI represents content owners, such as the RIAA and the MPAA, in finding and reducing piracy online. Because this process necessarily involves collecting information about private individuals, I was asked to investigate and determine that the information collected from online computing devices was adequately safeguarded and protected.

15. I am currently engaged as the Principal consultant with a large biomedical device firm in a one-year analysis of the security of their products. In particular, medical devices were for some time not considered significant threats in terms of computer security. However, recent demonstrations by security researchers of the various ways in which a malicious individual might harm a person hooked up to a medical device has shifted the thinking in the industry. Accordingly, Harbor Labs has been engaged to assist this company in the analysis of their products, their process, and their future roadmap in order to ensure that patients are not harmed. This evaluation, under my direction, is analyzing design documents, cryptographic protocols, hardware, and a broad range of additional resources in order to expose as many potential problems as possible for remediation. To-date, we have found a very serious vulnerability based on what is known as a “buffer overflow” attack. Had this critical error gone unnoticed by the manufacturer, malicious persons or organizations might have exploited it for harming patients, potentially with fatal results.

16. Beyond evaluating their current products, I am providing ongoing consulting services to this same biomedical device firm as they attempt to improve and refine their systems’ security. This work includes approaches for authentication of devices to networking systems, software to devices, and so forth based on cryptographic protocols.

17. I have also been engaged by another medical device manufacturer to consult with them on their security designs. I will be working with their design teams to identify threats (current and future) to medical devices, evaluate their proposed approaches to solving these problems, and guide them in their ongoing design and implementation.

18. In 2014 I received an appointment as a Lecturer at Johns Hopkins University and in 2015 I advanced to an Adjunct Associate Research Scientist. My responsibilities at Hopkins include teaching classes, mentoring students, and conducting research. More specifically, I currently teach the Network Security course for which I created the curriculum from scratch. As part of this curriculum, I designed a novel experimentation framework for allowing students to both build and attack security protocols. The course covered topics ranging from cryptography and access controls to network architecture and user psychology.

19. One of the components of the students' lab work is to create a protected sandbox for running untrusted code. The sandbox must provide access to the system in a manner that cannot be exploited. Conversely, the other half of their assignment is to design exploitative code that attempts to bypass and/or neutralize the protections of the sandbox environment. This experimental framework enables the students to learn about creating, identifying, and neutralizing malware such as viruses.

20. In addition to my course instruction, I also mentor Masters students at Johns Hopkins in their capstone projects. These projects include networking security and privacy concerns across a wide range of technologies including iOS security, BitCoin, SSL vulnerabilities, and Twitter botnets. These are all contemporary issues in practical computer security.

21. One group of students and I, for example, investigated the known Heartbleed vulnerability in certain versions of OpenSSL. Under my direction, the students created a vulnerable server to test. Once they were able to re-create the known vulnerability, they explored other ways of testing and finding vulnerabilities of the same sort using, for example, fuzzing.

22. Another student performed an analysis on “bots” in social media such as Twitter. Twitter relies on advertising to make money as the individual users are not charged for their accounts. This advertising process is based, in part, on identifying “influential” individuals (i.e., individuals with a large number of friends). Unfortunately, “bots” are computer programs that can act like a real person on social media sites. Individuals will sell buyers an arbitrary number of “friends” that are, in fact, just bots. My student and I created an approach for mapping out these so-called “botnets” in a novel way that may be useful in deterring such botnets. We are currently working on a draft of this research to be submitted for publication.

23. Based on my technical education, and my years of professional experience as an engineer and research scientist, I have specialized knowledge in the field of computer security, network security, secure communications, cryptographic operations, and software architecture that will/may assist the Board.

24. I have been retained by counsel for Leon Stambler to review materials related to this IPR, and to render opinions on whether certain items anticipate or render obvious specific patent claims.

The ‘302 Patent

25. According to its face, U.S. patent 5,793,302 (‘302) to Leon Stambler was filed November 12th, 1996 and issued August 11th, 1998. Also on the face of the patent, it identifies the ‘302 as being a continuation of several previous patents, the earliest of which is dated November 17th, 1992. This patent, entitled “Method for Securing Information Relevant to a Transaction,” discloses authentication of parties and information in a transaction system. ‘302 at Abstract.

26. Counsel has informed me that the only independent claim under review in this IPR is claim 51. This claim identifies a method for authenticating a transfer of funds from one account of a first party to an account of a second party. However, not just the funds are authenticated, but at least one of the parties’ identities is also established by a credential issued by a “trusted” party. ‘302 at 33:15-21.

27. The authentication of the funds transfer is achieved by first receiving the funds transfer information, then generating a “variable authentication number” (VAN) using some portion of the received information, determining whether the funds transfer information is authentic using the VAN (and credential information), and then actually transferring the funds if the transfer information is determined to be authentic. ‘302 at 33:22-35. The complete text of this claim is reproduced below:

51. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, the method comprising:

receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount;

generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;

determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and

transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

28. The term “Variable Authentication Number” is not a term of art. To my knowledge, I have never used it in my professional career, nor have I seen this term used outside of this patent.

29. These four steps of claim 51 appear in the specification in the embodiment of authenticating a check to be cashed. This embodiment describes a recipient attempting to cash a check from the originator. In this embodiment, the check has already been written and issued with a VAN attached by the originator. ‘302 at 4:2-5:34. The recipient has also already presented this check to his or her own bank for cashing. ‘302 at 5:55-6:45.

30. In accordance with the first step of claim 51, the originator’s bank receives the funds transfer information from the recipient’s bank (i.e., the transfer of funds from the originator’s bank account to the recipient’s bank account as indicated by the check). ‘302 at 6:43-45. The transmission includes the originator’s TIN, or tax identification number, that in addition to identifying the account, also is credential information. The originator’s bank uses the originator’s TIN in order to retrieve the originator’s file and information necessary to derive a “coded PIN.” ‘302 at 6:46-55, 11:48-49.

31. How the originating bank validates the funds transfer associated with the originator’s issued check depends on the embodiment. In one case, it decodes the VAN, somewhat similar to decrypting an encrypted piece of information. It uses the originator’s coded PIN with the TIN to generate what is called the “joint key.” This joint key, in this embodiment, is capable of decoding the VAN,

allowing the originating bank to validate the funds transfer information. ‘302 at 6:46-7:20.

32. However, in another embodiment, the originating bank uses the joint key to *regenerate* the VAN. This is a common approach in computer science to authentication with “one-way function” such as hashes. A one-way function is so-called because it cannot be decoded or reversed. To validate the correctness of information using a one-way function, the recipient also hashes the information and compares the generated hash with the transmitted hash. If they match, the information is presumed to be unmodified. Similarly, in this embodiment, which matches the claim limitations of claim 51, the originating bank uses the joint key and the transfer information to regenerate the VAN. If this VAN, and the VAN transmitted with the check match, the check is presumed to be unaltered. ‘302 at 7:12-16.

33. This second embodiment matches the second and third steps of the method of claim 51, namely, generating a VAN using the funds transfer information, and determining whether the funds transfer information is authentic using the VAN and credential information.

34. The originating bank then fulfills the last step of the method of claim 51 by transferring funds according to the transfer information if the VAN was determined to be authentic. ‘302 at 7:28-30.

Person of Ordinary Skill

35. I am informed by counsel that many of the issues before me in this matter, like obviousness for example, must be considered from the point of view of one of ordinary skill in the art at the time of the '302's priority date (1992). I agree with Patent Owner's statement in the Preliminary Response that a person of ordinary skill in the art for the patents-in-suit would likely have the following educational background and experience: (1) undergraduate education in mathematics, physics, computer science, electrical engineering or similar technical subject; and (2) either post-graduate education in networking, cryptography, or other discipline encompassing information theory, or equivalent experience with applications involving communication of financial, military, medical or similarly sensitive data over secure and non-secure networks. Although I was not a person of ordinary skill in the art in 1992, I am familiar with the state of the art at that time by training and research.

36. For example, in my training in computer science, I was taught the development of the art in the normal order of my courses. In particular, it is expected that I become familiar with "seminal" papers and pivotal moments in computer science in order to understand the state of the art today. Many of my classes included materials written in the 70's, 80's, and 90's. In one of my computer security courses, for example, I was assigned to read "Using Encryption

for Authentication in Large Networks of Computers,” which is dated 1978. Another assignment from the same course was the paper “Reflections on Trusting Trust,” which is dated 1984. These papers are examples of works considered foundational in computer security and still affect our views on these topics today.

37. One of my textbooks during my college years was “Security Engineering,” by Ross Anderson. In his chapter on cryptography, which is the science and art of creating and breaking ciphers, Anderson provides a historical background that begins with Julius Caesar’s cipher from more than two-thousand years ago. Anderson walks through the development of cryptography during the 1800’s, including how banks authenticated funds transfers sent over telegraph wires. From there, he continues into the modern age with the development of the systems we use today such as public and private key pairs.

38. I use this same textbook today in teaching my own security course (albeit with a newer edition), and I also guide my students through the history and development of Network Security.

39. Since graduating with my Ph.D., I have also spent countless hours researching technologies, past and present, in my consulting work. I have, for example, reconstructed viruses from the mid 90’s, studied anti-virus technologies from 1990-present, and even examined source code from early anti-virus

manufacturers. I have also re-created software from that time period, and setup operational demonstrations of technologies from that era.

40. Nothing in these preceding paragraphs should be construed as the entirety of my basis for understanding of the art, and a person of ordinary skill in the art, in 1992. Rather, these examples are given as illustrations only.

Applied Claim Construction

41. I am not a lawyer, but I have submitted expert reports in patent litigation cases, and declarations in other IPR proceedings. From my experience, and as informed by counsel, I understand that in many patent litigation cases, the court will provide a “claims construction.” I understand that such claims are construed or defined by this construction process, and must be interpreted accordingly.

42. I also understand from experience and as informed by counsel that in many IPR proceedings, the terms are not subjected to a normal claims construction process. Instead, terms are assumed to have their “broadest reasonable interpretation,” or BRI.

43. However, I understand from counsel that in this IPR proceedings, the ‘302 patent has already expired. Accordingly, the BRI does *not* apply to the terms of the ‘302 patent. I understand that terms in the ‘302 patent must, therefore, be interpreted according to traditional construction. I also understand that there is a

dispute between the petitioner and patent owner as to the scope of certain terms within the claims.

44. I understand from counsel that the Patent Owner has asserted that a “credential” should be construed as “a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party.” I understand that this construction is largely adopted from a court construction in five prior patent litigation cases involving the ‘302. Ex. 1018, at 2.

45. I also understand from counsel that the petitioner has not offered a competing construction. Nevertheless, counsel has also informed me that the PTAB did not address this construction issue in its decision to move this IPR matter forward.

46. I am of the opinion that the petitioner’s construction is reasonable and supported by the specification of the ‘302 patent. For example, the specification lists “identification cards” as an example of a credential, which is clearly information obtained from a trusted source that is presented for purposes of identifying the presenting party. I could find no examples of a credential within the ‘302 specification that did not meet this construction.

47. Counsel has asked that I perform my evaluations of the issues at hand using the above construction except when adopting petitioner’s implied

construction is necessary to refute or critique their arguments. It will be clear from context whether I am using the Patent Owner's construction or the petitioner's implied construction.

48. I understand from counsel that the petitioner has offered no construction for "information for identifying the account of the second party." I also understand from counsel that Patent Owner also believes that no construction is necessary. Nevertheless, to the extent that the petitioner believes that the plain meaning of this term is the name of a party, I disagree.

49. In the first place, the specification uses account-identifying information such as a TIN (tax identification number). '302 at 6:22-26 and 6:46-55. I am aware of no examples from the specification wherein the name of the party is considered identifying of the account.

50. Moreover, whereas in the '302 examples a TIN identifies a particular account, a name does not identify an account. Consider a name like "John Smith." Such a name might apply to many people, and each individual "John Smith" may have multiple accounts whereas a TIN uniquely identifies the party (and in the '302 examples, uniquely identifies an account).

51. Accordingly, the term must be construed as "information that is used to identify an account of the second party." Three other courts have adopted this construction. Ex. 1013, at 23-24; Ex. 1014, at 13; Ex. 1015, at 41-43

52. I understand from counsel that the patent owner is not contesting petitioner's construction of the term VAN, but that he is contending that additional construction is required on the term "coding," which is used to create the VAN.

53. Within the patent specification, coding is performed by a hardware component or some portion of a computer program. '302 at 3:30-36 and Fig. 1. The specification goes on to say that the coding is performed by an entity that uses a "known algorithm" (such as DES). '302 at 3:38-39.

54. I also understand from counsel that during prosecution, the patent owner (then applicant) stated that the newly added claims (which became the issued claims) describe transactions that are electronic and only electronic, where funds transfers are credited and debited automatically. Ex. 1011 at 306-07

55. Based on the specification and file history, I believe that the VAN must be coded using an entirely electronic device that is either a hardware component, or a computer running a functional block of a computer program to transform information by applying a known algorithm.

56. I understand from counsel that patent owner seeks to have the term "error detection code" construed as "the result of applying an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the original information can be detected without complete

recovery of the original information.” I also understand from counsel that petitioner is not seeking a construction of this term.

57. I believe that this construction represents a correct understanding and application of this term to the patent claims.

58. I understand from counsel that patent owner believes that the correct construction of the “secure” phrase in claim 56 is that “the VAN1 being used to verify or determine that the at least a portion of the information stored or contained in the credential is associated with the at least one party.” I also understand that petitioner is not seeking a construction of this term.

59. A previous court endorsed and approved this as an agreed construction. Ex. 1017, at 2.

60. I believe that this construction is the only possible way that the VAN1 can be used in claim 56 as I will describe in subsequent paragraphs.

61. I have been informed by counsel that the legal standard for “enablement” is that the specification must provide enough written description for a person of ordinary skill in the art to implement the claimed invention without undue experimentation and/or with predictability of success. I also understand that it is improper to add additional limitations into a claim based on embodiments in the specification; at the same time, counsel informs me that claims cannot be of a broader scope than the invention described by the specification.

62. After reviewing the specification, I am of the opinion that the limitations of claim 51 must be performed by a single entity. Otherwise, there would be insufficient written description to enable the claim. Said another way, a person of ordinary skill in the art would not have sufficient written description in the specification to enable implementing claim 51 such that multiple entities divide up the performance of the comprising steps. To stray from the specification in this fashion would require undue experimentation and with little predictability of success.

63. As stated previously, claim 51 sets forth a method comprising four steps: receiving funds transfer information, generating a VAN, authenticating the funds transfer information using the VAN and credential information, and transferring the funds if the transfer information is determined to be authentic.

64. The sole support for this claim 51 in the specification is the funds transfer embodiment I previously discussed. In that embodiment, all four steps are performed by the originator's bank. The bank first receives the funds, generates a VAN, compares the VAN against the VAN on the funds transfer information, and transfers the funds if the comparison fails.

65. Such an embodiment is easy to understand and straightforward for a person of ordinary skill in the art to implement. Each step is a clear precursor for the next.

66. If multiple entities perform these steps, there is information deficient about how to implement the claim. For example, if one entity receives the funds transfer information, and another entity then determines the VAN, the claims and the specification do not describe how the funds transfer information gets from the first entity to the second. Or, if one party performed those first two steps, but another party determined if the VAN was authentic, the patent says nothing about how the VAN is transmitted *and* how it would be transmitted *securely*. Because the VAN is an authentication number, it would have to be transmitted securely (without significant vulnerability from attacks) from the party generating the VAN to a party determining if the VAN is authentic.

67. Cryptographic protocols, including authentication protocols, are notoriously difficult to get correct. For example, the Needham-Schroeder protocol, published in 1978, was found to have a weakness (vulnerable to a “replay attack”) in 1981. It should be noted that this protocol was developed by two people with Ph.D.’s and a wide number of years of experience. In other words, two individuals that were *far above* one of *ordinary* skill in the art. For a person of ordinary skill in the art to know how to alter claim 51 to be performed by multiple parties, this hypothetical individual would have to create a workable cryptographic protocol to keep the authentication secure. This is particularly so when no measures are

described to protect the communication between two entities from malicious eavesdroppers and attackers.

Preliminary Discussion of Davies

68. The Petitioner relies heavily upon the book, “Security for Computer Networks,” by D.W. Davies and W.L. Price (“Davies”) for almost all of its arguments. The Davies reference is a 1989-era textbook discussing a wide range of security issues and solutions including a history of cryptography, ciphers contemporary to 1989, how to manage encryption keys, and how to identify a party. As is true with most textbooks, the goal of Davies is not to disclose full systems with all necessary details; rather, it teaches key principles and concepts to students using simplified or pedagogical systems for context and clarity. Students thus instructed are then better prepared for dealing with the real systems they encounter in the real world. Davies is, itself, contains the sub-title, “An *introduction* to Data Security in Teleprocessing and Electronic Funds Transfer.”

69. Chapter 10 of Davies is entitled, “Electronic Funds Transfer and the Intelligent Token.” This part of the book discusses a wide range of issues related to electronic commerce. Petitioner relies primarily on a discussion of electronic checks (“electronic cheques”) and their use in Point-of-Sale (“POS”) and ATM systems.

70. Davies opens the discussion of electronic checks by comparing them *in terms of trust* to paper checks. It says, “[t]oday, many [paper] payments are made without reference to a bank, for example by means of a [paper] cheque.” Davies connects this to an electronic equivalent saying, “There will in future be many occasions when payment through a communication network is useful but reference to a bank is not convenient.” Then, addressing issues of trust explicitly, it adds, “[f]or example, an on-line information service charges a fee but a caller does not have to be a *known subscriber* to the service; he can be *anyone* who ‘presents a bank card...’ which requires *some trust between the parties*.” Davies at 328, emphasis added.

71. In the subsequent paragraph, Davies lays out an electronic check that is basically a few data fields electronically signed by a hierarchy of parties. The data includes the bank’s name, the customer’s name, the amount of payment, the payee’s identity, and so forth. One part of the check is signed by an unidentified key registry, another portion is signed by the bank, and (once the amount and payee portions are filled out) the remainder is signed by the customer. Although Davies does not say it explicitly, the recipient of the check can only trust the funds transfer encoded therein if he or she also trusts the registry and verifies the chain of signatures. Davies also does not describe the registry in detail but suggests that it could be the central bank of a country as an example. Davies at 328-329.

72. However, even if the registry is trusted, it should be noted that what is authenticated by this hierarchy of signatures is funds transfer information, not the individual presenting the check. As Davies explicitly disclosed in this same section, the electronic check technology is aimed at systems where the issuer of the check “can be anyone.” So long as the transfer of funds is authentic, the service does not care about the identity of the originator. Davies at 328.

73. In the paper world, checks have the same function. In fact, when businesses are concerned about the issuer of a check, they ask for another credential (such as a photo-ID) to identify the person.

74. Describing it like an “electronic chequebook,” Davies suggests that “private” customers could use an electronic device or “intelligent token.” This device would store the customer’s private electronic key used for signing the checks described above. This token is protected by a customer PIN that is entered either directly on the device if it has its own PIN or through any compatible terminal. If a customer issues a check using this device, the device (after correct PIN entry) generates the check and signs it before transmitting it to the recipient. From the perspective of the recipient, it makes no difference for verification purposes if the check was signed by a token or not. Davies at 329.

75. After discussing the “electronic cheque,” Davies discusses how point-of-sale (POS) payments can be made using this technology. The payment

mechanism is divided into an “online” mode and an “offline” mode. The online mode assumes that the POS terminal of the merchant can immediately submit the received check for processing by the originator’s bank. In the offline mode, the check is submitted later, perhaps in “batches” of received checks. Nevertheless, in both online and offline mode, the check is presented in the same way. Davies at 330. In an earlier segment of the book, Davies described an online POS mechanism using public keys. Davies at 311-324. This approach is not the same as the check example and was not matched to claim limitations in the petition.

76. Davies also discloses that the “intelligent token” used in issuing checks can also be used with POS terminals and ATM machines. Although there are some similarities, the two examples are separate and distinct. It should be noted that the ATM example is left not fully specified by Davies, although this is not uncommon for textbooks (e.g., “left as an exercise for the reader”). The ATM description, for example, does not say to whom the electronic check should be written. It does, however, make it clear that the fields of the electronic check should be adapted to their different uses and that a “transaction type” field can indicate whether it is being used for ATM, “customer cheque,” and so forth. Davies at 330-331. Certainly if the “transaction type” field is “ATM” that there would be no need to write “payee identity” into the electronic check.

Secondary References

77. Meyer is a textbook from 1982. As with Davies, it describes a number of different aspects of security including cryptography. Also of note is that Davies references Meyer.

78. Nechvatal is a publication by the National Institute of Standards and Technology (NIST). This paper, from 1991, reviews public-key cryptography systems and public-key cryptography technology from that time period. In particular, Petitioner notes that Nechvatal identifies a “root” certificate authority and also hashes a message before signing.

79. U.S. patent 4,868,877 to Fischer (“Fischer”) discloses a public-key cryptographic system. One of the key elements of this system identified by the Petitioner is a hierarchy of signing authorities. That is, a public key is signed by a chain of keys that can all be verified up to a “root” authority.

80. U.S. patent 4,993,068 to Piosenka (Piosenka) outlines a system for generating credentials for a user. The user submits information for identification, the system verifies this information, and then issues a credential for the user.

Detailed Analysis of Errors by Petitioner

81. In the petition, MasterCard asserts that “Davies teaches each and every limitation of claims 51, 53 and 55 of the ‘302 Patent...” Further, a claim chart is included that Petitioner further asserts shows this teaching. Nevertheless, I have noted several errors that I will identify in the subsequent paragraphs. To

evaluate the anticipation assertions, I have applied the principle that for prior art to anticipate, a person of ordinary skill in the art must be able to perceive that it discloses the entirety of a claimed invention within that single reference, arranged as in the claim. Note that my pointing to particular errors does not mean I necessarily agree with or endorse assertions not explicitly addressed.

82. In the petition's claim chart, MasterCard identifies two separate examples for meeting the first part of the preamble of claim 51 ("51preA"). This limitation reads: "A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party."

83. Under the heading "Example I," the petition cites to a section in Davies that strangely has nothing to do with electronic funds transfer. This is clear from the paragraph just preceding that the discussion revolves around current (not proposed) mechanisms for paying (cash, cheques, and credit cards). Within the pages quoted by the Petitioner, it is clear that this is manual and not electronic checking ("The big practical disadvantage of the cheque system is its slowness...", "The physical sorting of cheques to return them to their payer's banks...", "In principle, the whole system could work without paper as soon as...", "The security of the cheque mechanism depends on the manual signature", and most explicitly, "The paper cheque with its manual signature is not an ideal subject for automation..."). Davies at 285-286.

84. In the second example (“Example II”), Petitioner does cite the electronic checking mechanism that I described in my treatment of Davies. While the electronic check does deal with the electronic transfer of funds, it does not identify an account associated with a second party. The payee’s name is identified but not his or her account. Davies at 328-329. When the check is submitted, the bank must determine the account of the individual, and which account is often ambiguous without information beyond the recipient’s name.

85. The next part of the preamble (“51preB”) reads: “a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret...”

86. For this part of Claim 51, the Petitioner again presents two examples labeled “Example I” and “Example II.” However, the Example I from this section, which describes a generic key-registry system for authentication of keys, is completely divorced from Example I of the earlier 51preA limitation. If the Petitioner intended Example I elements to connect with other Example I elements, then it clearly fails here. If, on the other hand, Petitioner intends to link unrelated elements together, it fails to identify the rationale for that combination. Davies never ties together paper checks and key registries and neither does the petition.

87. Example II in 51preB does appear to be related to Example II of 51preA. Petitioner cites to Davies discussion of authenticating the electronic check by means of a key registry.

88. The narrative text presents Petitioner's apparent theory about what the "credential" is in 51preB. It states, "Davies further describes that the *public key* ('non-secret information') of a sender... is contained in a *certificate* ('credential')..." In the next paragraph the petition argues that "Davies teaches that the *electronic check* serves as a certificate ('credential') for the customer that includes the customer public key ('non-secret information')..." It is not clear if Petitioner intended these to be two parts of the same argument or two separate arguments. Nevertheless, it fails to meet the claim limitation in either case.

89. First, the electronic check cannot be the credential. The check is not presented for purposes of establishing or determining the identity of the party. The check may be presented by anyone and, so long as it is signed with the appropriate cryptography, it is accepted for funds transfer. In fact, the motivating example in the electronic check in Davies is an "offline information service" that does not need "known subscribers." It is a service that responds to "anyone." Davies 328-330. Moreover, there is no evidence in Davies that a check is a "certificate."

90. The other proposed credential here is a "certificate" issued by the registry. This is incompatible with the electronic check embodiment because the

only certificate issued by the registry is to the bank and not one of the two parties. As Petitioner has only identified the public keys of the sender and/or receiver as the (non-secret) credential information, there is no certificate issued by the registry that meets this claim limitation.

91. Although the Petitioner only identified the key registry as the trusted entity, should they try to argue that the bank is a trusted entity, Davies does not disclose the bank issuing a certificate to the check originator. The bank signs the public key in the electronic check, but does not issue a certificate.

92. The next limitation of the '302 patent (51a) reads: "receiving funds transfer information including at least information for identifying the account of the first party and information for identifying the account of the second party, and a transfer amount."

93. At this point, the Petitioner includes only a single example without appearing to tie it to any of the previous examples. The claim chart jumps to a different embodiment at this point, namely cashing an electronic check at an ATM. That Davies uses the same electronic check mechanisms described for the previous elements is not in dispute. Nevertheless, in describing the standard use for the electronic check Davies states, "The transaction type [field of the electronic check] is provided in order to use this same format *for other purposes*." Davies at 329, emphasis added. When introducing the ATM example, Davies starts calling the

check “a message” and states, “To differentiate these messages and provide for even wider use, the [electronic check format] includes the *transaction type* which denotes a customer cheque, ATM request, interbank payment, payment advice and so forth.” Davies at 331, original emphasis.

94. The ATM example in Davies is not given in great detail. The exact formatting of the check is not given because, for example, a payee field is no longer needed. Even the “date and time” field would not be absolutely necessary anymore because the ATM will keep its own time stamps. In other words, exactly how the electronic check description of Davies ties in with the ATM is not explicitly presented.

95. To the extent that the Board believes that the electronic check and ATM elements of Davies constitute a single disclosure, it is deficient for another reason. Petitioner identifies the “intelligent token” of the ATM example as the component that “receives funds transfer information.” For this to meet the claim limitation, the token must receive information identifying the account of the first party, information identifying the second party, and a transfer amount.

96. The problem is Davies does not disclose *what* the token receives. In the “electronic checkbook” example, Davies simply says that the check (generated by a terminal) is “...sign[ed] with the aid of the token...” without describing how it is signed. Davies at 329. If, for example, the terminal just sends a “blob of

bytes” to be signed, the token does not receive the funds transfer information in any intelligible form. It simply signs bytes without knowing what those bytes mean.

97. However, Davies does suggest that the smart token “can” record the transactions it makes. Davies at 329. It is possible that such a token is aware of what the different fields in the check mean. But if that is true, the token would not need to have the customer input things like the “customer identity” or any information for the account. Truly, if the token has this information loaded internally then it only need receive “payee information” and “transfer amount” in order to complete a check. There would be no reason to receive account information associated with the sender.

98. Davies is even less clear with regards to the ATM example, as it simply states, “The customer’s request is formed into a message and presented to the token.” Davies at 330-331. It does not say what form that “request” or “message” takes. If we have a “blob of bytes,” the token does not know if it is an ATM request or an electronic check. It simply receives bytes and signs them. If the token is smart enough to be aware of the ATM transaction, then it would only need to receive the transfer amount.

99. Part of the reason that Davies is so vague about the precise details of this system is because it was not a real-world system. All of this is conjecture on

Davies' part about what *might* happen in the future. Note that Davies closes this section about the ATM with the following comment: "*If* public key signatures come into use first in payment systems, the financial institutions *will* establish key registries... In this way the operation of key registries *may* become a function of financial institutions." Davies at 331, emphasis added. Without the further details that come from an actual invention, it is impossible to know what the Davies' token was and was not receiving.

100. Even if we assume that the token is receiving funds transfer information, in the case of the ATM, there is no reason to believe that it is receiving information identifying the account of a second party.

101. And finally, as already mentioned, the '302 patent only enables having a single entity practice all the steps of claim 51. Even if the token did perform the steps of receiving and generating, the token does not perform the steps of determining the authenticity that follow.

102. After receiving the funds transfer information, the '302 patent requires (51b): "generating a variable authentication number (VAN) using at least a portion of the received funds transfer information" and (51c): "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information..."

103. The petition addresses these two elements together and, again, introduces two examples (“Example I” and “Example II”) for each one without tying them back to previous examples. In all cases, however, Petitioner relies on the electronic check as the credential. As I have previously explained, the check cannot be the credential. In this segment, Petitioner states that the customer’s public key is signed by the bank, implying that the bank is the trusted party. This is contrary to their earlier assertion that the key registry was the trusted party. I have previously addressed this as well.

104. And finally, as already mentioned, the ‘302 patent only enables having a single entity practice all the steps of claim 51. Even if the token did perform the steps of receiving and generating, the token does not perform the steps of determining.

105. The final step of Claim 51 of the ‘302 patent is, “transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.”

106. This limitation fails for numerous reasons previously discussed.

107. First, in the ATM example, there is no transfer to the account of the second party. The money is subtracted from the customer’s account and given to them in cash.

108. Second, the '302 patent only enables having a single entity practice all the steps of claim 51. Even if the bank did perform the steps of determining and transferring, the bank does not perform the steps of receiving and generating.

109. For any one of these reasons, Davies does not anticipate claim 51. I understand that these reasons also prevent a finding that Davies anticipates claim 53.

110. Petitioner cites claim 51 as obvious because of Davies in view of Meyer. However, as the petitioner does not rely on Meyer to supplement gaps within Davies identified above for the limitations of Claim 51, I need not re-evaluate these claims.

111. However, Petitioner does rely on Meyer in Claim 56 exclusively. This claim is dependent on Claim 51 and, as such, inherits all of the deficiencies that I have addressed for that claim.

112. Claim 56 has two parts. The first part (56a) reads, "The method of claim 51 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party."

113. Petitioner points to a discussion from Meyer about protecting private key data stored in an intelligent token by combining it mathematically (XOR) with the PIN. This, however, ignores that the claim requires “credential information” to be protected and the credential information must be “non-secret.” The private key protected by Meyer is, in fact, secret and not-disclosed. Meyer at 591.

114. I understand from counsel that the Petitioner must present a reason to combine. Counsel has informed me (and I agree) that it is not sufficient that art is “similar.” To the contrary, it is my understanding that two very similar pieces of prior art may actual represent a motivation to *not* combine. If the prior art is self-contained and does not seem to recognize any flaws or deficiencies, I understand that this would actually discourage combinations with other art as it is already seen to be complete.

115. Based on my understanding of these legal principles as explained by counsel, the Petitioner must demonstrate that there were reasons to look for extending or modifying prior art with another reference. However, in my reading of the petition, I cannot find any such explanation. Petitioner says that all of the elements would have yielded a known result without any argument for why a person of ordinary skill in the art would have sought out those results.

116. The declaration of Mr. Diffie asserts similar conclusions without explanation. For example, Mr. Diffie states, “Thus, these references in their

similar purpose of dealing with financial transactions and services, and overlapping teachings, confirm a motivation to combine Davies and Meyer...” Diffie Decl. at 112. I understand from counsel (and I agree) that this is not sufficient motivation to combine and no additional rationale is given in Mr. Diffie’s declaration.

117. Although counsel informs me that it is not my burden to *affirmatively* demonstrate that there is no motivation to combine, I do note that both Davies and Meyer are textbooks. Davies cited to Meyer and, thus, is aware of Meyer. Davies does not seem to feel that additional information is necessary from Meyer or it would have included it.

118. For the combination of Davies and Meyer with Nechvatal, Mr. Diffie does offer a possible technical motivation to combine. In particular, he asserts that one would have been motivated to combine Nechvatal’s hash-then-sign teaching with Davies because Nechvatal explains that it would be more efficient to perform signatures in this fashion.

119. I disagree with Mr. Diffie, however, that this would be motivation to combine these references. The Davies reference already discusses the possibility of hashing and then signing *when the message to be signed is large*. Davies at 264. However, the electronic check messages described in the embodiments are not large messages and would not see increased efficiency for signing the message.

This was acknowledged by Mr. Diffie himself. Diffie dep. 32:20-33:21; 37:18-38:22.

120. Similarly, Mr. Diffie also provides a motivation to combine Fischer and Davies. Fischer describes a hierarchy of key signing so that a recipient can validate a sender's key so long as the chain of signing eventually hits a trusted party. Fischer also describes having one authority potentially limit the power of a lower authority. I will identify and address each of Mr. Diffie's motivations below.

121. First, Mr. Diffie argues that Davies "does not explicitly disclose that the recipient may authenticate the sender's public key before using it to verify the message signature." Diffie decl at 158. What Davies does say, however is that, "The second section of the cheque contains the customer identity and his public key, signed by the bank and therefore verifiable using the [bank's public key included in the cheque]." Davies at 328. Accordingly, I do not see that one of ordinary skill in the art would have thought another reference was necessary.

122. Second, Mr. Diffie states that Fischer's "counter signature" that limits what a lower authority can approve is valuable in limiting fraud. Diffie decl at 159-160. However, he does not explain why one would be motivated to combine that teaching with Davies. Davies does mention corporate customers and interbank transactions briefly, but the primary example is personal checks. The POS and

ATM embodiments, which are the examples cited by Petitioner, are also directed at the personal customer. There is no reason to limit the purchasing authority of personal checks by the bank, and any such limitations are usually placed by the receiving entity instead. Davies at 328-331.

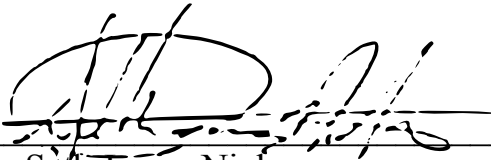
123. The combination of Piosenka and Fischer (with Davies) is conclusory. Petitioner appears to make no arguments other than there is overlap and similarities between the systems. Mr. Diffie also focuses solely on the similarities and how the two systems might work together. I understand from counsel (and I agree) that this is not sufficient to motivate the combination.

124. I also note that there would be technical barriers to Mr. Diffie's suggestion that, "combining Fischer with Piosenka would allow different identification systems in Piosenka to issue user credentials that including information of the respective identification systems..." Diffie decl. at 176. Not only does he fail to give a motivation for such a combination, but he fails to explain how such a combination would be achieved.

For these reasons, Davies in combination with the secondary references does not render obvious any of claims 51, 53, 55 or 56.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Dated: October 20, 2015


Seth James Nielson

HARBOR LABS

SOFTWARE & NETWORKING EXPERTS

Seth James Nielson, Ph.D.

410.497.7384

seth@harborlabs.com

Profile

I am a Principal at Harbor Labs with specialties is network security, network communications, software architecture, and programming languages. With over a decade of industry and academic experience providing software development, software reviews, security reviews, cryptographic analysis, and technical training, I enable clients to succeed in their technology projects. I also have extensive experience as a technical expert having supported legal teams with analysis and insight on patents, DMCA, code theft, and trade secrets. In addition to providing numerous code reviews, expert reports, and technical analyses, I have been deposed several times and have testified at trial.

I completed my Ph.D. at Rice University in 2009 where my thesis investigated questions of security and anonymity in peer-to-peer (P2P) systems like BitTorrent. In addition to my professional work at Harbor Labs, I am an Adjunct Associate Research Scientist at Johns Hopkins University where I teach network security classes, mentor student capstone projects, and engage in academic research.

Education

<u>2009</u>	<i>Rice University</i>	Ph.D. in Computer Science
<u>2004</u>	<i>Brigham Young University</i>	M.S. in Computer Science
<u>2000</u>	<i>Brigham Young University</i>	B.S. in Computer Science

Academics and Research

<u>12/2014-Present</u>	<i>Johns Hopkins University</i>	Adjunct Associate Research Scientist
	Teach graduate level courses on network security	
	Advise student capstone projects	
	Engage in academic research	

<u>1/2014-12/2014</u>	<i>Johns Hopkins University</i>	Lecturer
	Teach graduate level courses on network security	
	Advise student capstone projects	

Industry Positions

<u>2011-Present</u>	<i>Harbor Labs</i>	Principal
<u>2005-2011</u>	<i>Independent Security Evaluators</i>	Senior Security Analyst
<u>2005</u>	<i>Google</i>	Summer Intern
<u>2001-2003</u>	<i>Metrowerks (Formerly Lineo, Inc.)</i>	Software Engineer II

Academic Awards

Brown Fellowship
John and Eileen Tietze Fellowship

PHONE

FAX

WEB

3 Thornhaugh Ct., Baltimore, MD 21208

410-415-3305

410-264-2406

www.harborlabs.com

Patents

Co-inventor: Orsini, R. 2014. *Systems and methods for security data in motion*. U.S. Patent 8,745,372 filed November 24, 2010 and issued June 3, 2014.

Co-inventor: Orsini, R. 2014. *Systems and methods for security data in motion*. U.S. Patent 8,745,379 filed August 20, 2012 and issued June 3, 2014.

Co-inventor: O'Hare, R. 2014. *Systems and methods for security data*. U.S. Patent 8,677,148 filed January 27, 2012 and issued March 18, 2014.

JHU MSSI Capstones

Research on the Heartbleed Vulnerability, Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu (May 2015)

Buying Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter, Richard Eaton (May 2015)

Security Techniques for Developing iOS Applications, Kartik Thapar (February 2015)

Privacy and Threats in Bitcoin, Jie Feng, Jianxiang Peng, Likai Zhang (January 2015)

Publications

Seth James Nielson, *PLAYGROUND: Preparing Students for the Cyber Battleground*, Submitted to the Journal of Computer Science Education.

Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, *Guidelines for Source Code Review in Hi-Tech Litigation*, Harbor Labs White Paper (September 2013)

Seth James Nielson, *Reintroducing Pylogical*, BYU SEQuOIA Technical Report, (March 2012)

Seth James Nielson and Dan S. Wallach, *The BitTorrent Anonymity Marketplace*, arXiv Technical Report 1108.2718, (August 2011)

Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, *Building Better Incentives for Robustness in BitTorrent*, arXiv Technical Report 1108.2716, (August 2011)

Seth James Nielson, *Designing Incentives for Peer-to-Peer Systems*, Rice University Department of Computer Science Ph.D. Thesis (2010)

Seth James Nielson and Charles D. Knutson, *Design Dysphasia and the Design Patterns Maintenance Cycle*. *Information & Software Technology*, volume 48, number 8, pp. 660- 675, (August 2006)

Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, *A Taxonomy of Rational Attacks*. In *Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, New York, (February 2005)

Seth James Nielson, *OO++ Design Patterns, GOF Revisited*, Brigham Young University Department of Computer Science Master's Thesis (2004)

Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, *Attacks on Local Searching Tools*, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011)

Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Effective Bandwidth for Traffic Engineering*, in *Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, TX, (May 2001)

Selected Consulting and Industry Experience

7/2015-Present *Medical Device Security*

Client: Confidential

Overview: Ongoing security evaluation of medical devices from a major manufacturer

- Principal consultant for a one-year, multi-stage engagement
- On-site interviews and discussion with technical staff
- Evaluation of physical hardware and networks, design docs, etc.
- Confirmation of reported vulnerabilities
- Security recommendations for current and future products

10/2014-Present *Device Certification Consulting*

Client: Security First Corporation

Overview: Evaluate devices and software against regulatory requirements

- Evaluate products against HIPAA, FISMA, SOX, GLBA, NERC, ISO 27002 requirements

8/2013-11/2014 *Privacy Analysis in Forensic Data Collection*

Client: Center for Copyright Information

Overview: Ensure that private information in copyright abuse tracking is adequately protected

- Interviews with technical staff
- Analysis of design and policy documents
- Recommendations for improved privacy protection
- Public executive summary available: <http://www.copyrightinformation.org/wp-content/uploads/2014/11/Harbor-Labs-Executive-Summary.pdf>

7/2011-12/2011 *Automated Security Tools*

Client: Confidential

Overview: Development of automated tools for security testing

- Development of an automated, parallelized code coverage tool based on gcov
- Development of a tool for fuzzing iOS applications

8/2005-9/2011 *Development of Security-Related Software*

Client: Security First Corporation

Overview: Development of cryptographic library and sundry applications

- Technical lead of a secure communication library including prototype, design, and implementation
- Deployment of custom cryptographic library to filesystem encryption

- Hardware acceleration for cryptographic operations using CUDA and GPUs
- Development of custom cryptographic library for data at rest and data in motion

Summer 2005 *Security Intern at Google*

Overview: Development of a fix for privacy loss in the Google Web Accelerator

- Analysis of the security flaw
- Design and implementation of a solution to the problem

1/2001-9/2003 *Software Engineer II at Metrowerks*

Overview: Development of various applications for embedded Linux development

- Technical lead for the development of the SDK UI
- Technical lead for the development of a software update packaging system
- Technical lead for the development of a transparent remote script system

Technical Expertise

1/2001-Present *Software Development*

Languages: C, C++, Java, Python, Objective-C, Assembly

Targets: Applications, libraries, device drivers, simulators, networking stacks, graphics, server code, security code, pedagogical tools, utilities, automation, GUIs, intrusion detection systems, attack simulation technology

Toolkits: QT, Boost, Twisted, SWIG, test harnesses, CUDA

Platforms: Windows, Linux, iOS

9/2004-Present *Vulnerability and System Analysis*

Examples: Medical device security, Google Desktop Search (2004), crypto protocols, viruses, malware, passwords, cryptographic implementation, security policy viability, marketplace viability and risks of existing and future products

Tools: IDA Pro, port scanning, Formal cryptographic analysis tools, GCov and code coverage tools, fuzzing

1/2010-Present *Source Code Review and Analysis*

Samples: Antivirus software, firewall software, high-frequency trading algorithms, wireless protocol implementations, intrusion prevention software, email server software, document signature software

Tools: Understand, customized scripts

1/2010-Present *Technical Analysis of Intellectual Property*

Issues: DMCA and copyright

5/2010-Present *Technical Instruction*

Teaching non-technical professionals about relevant high-tech operations

Teaching technical professionals about technologies relevant to intellectual property

9/2011-1/2012 *Technical Project Management*
Projects: Secure communication application, automated fuzzing tool
Internal: Coding guidelines, manpower allocation, quality assurance
Customer: Requirements analysis, budget and scheduling, conflict resolution

9/2005-9/2011 *Cryptographic Library Development*
Algorithms: AES-GMAC, Shamir Key Splitting, Client-custom algorithms
Special: GPU-accelerated AES (CUDA), file system integration, FIPS certified

Expert Witness

3/2015-8/2015 *Afilias PLC v. Architelos Inc. and Alexa Raad*
Client: Afilias PLC
Counsel: Philip Hampton (of Haynes Boone)
Issues: Misappropriation of Proprietary Information
Technology: Domain name registrars, domain name anti-abuse
Status: Testified 8/2015, Deposed 6/2015

2/2015-Present *Sensus USA Inc. v. Certified Measurement Inc.*
Client: Sensus USA
Counsel: Rafael A. Perez-Pineiro, Javier Sobrado (of Feldman Gale)
Issues: Claims construction, IPR
Technology: Cryptography, certified measurements
Status: Declaration submitted

12/2014-Present *Chad Eichenberger v. ESPN*
Client: Chad Eichenberger
Counsel: David Mindell (of Edelson PC)
Issues: Declaration in support of amended claim
Technology: Privacy
Status: Declaration submitted

9/2014-Present *Fortinet Inc. vs Sophos Inc., et al*
Client: Fortinet
Counsel: Michael Niu, Jordan Jaffe, Kristen Lovin (of Quinn Emanuel)
Issues: Claims construction, IPR, Infringement, Invalidity, Non-infringement
Technology: Network security devices, anti-virus, anti-spam
Status: Deposed 10/2014; Tech tutorial for Court 12/2014

3/2014-Present *M2M Solutions vs Motorola Solutions, Telit Communications, and Telit Wireless*
Client: Telit
Counsel: David Loewenstein (of Pearl Cohen)
Issues: Collaborating expert on both patent infringement and invalidity
Technology: Authentication
Status: Deposed 6/2015

1/2013-8/2015 *Rmail limited vs. Amazon, Inc. and Paypal*

Client: RMail
 Counsel: Lewis Hudnell (of Colvin Hudnell)
 Issues: Patent infringement and validity
 Technology: Secure email, message authentication
 Status: Deposed 5/2013

9/2014-4/2015 *Microsoft v. Optimum Content Protection*

Client: Microsoft
 Counsel: Herman Webley (of Sidley Austin)
 Issues: IPR declaration
 Technology: Network security
 Status: Declaration submitted

5/2012-3/2014 *Via Vadis, LLC vs. Skype, Inc.*

Client: Via Vadis, LLC
 Counsel: Steven Taylor (of Whiteford, Taylor, Preston)
 Issues: Patent infringement
 Technology: Peer-to-peer networking

Litigation Support

1/2010-Present *Technical (Non-testifying) Expert*

Cases: More than twenty cases involving patents, DMCA, and other IP matters
Technologies: Firewalls, databases, electronic voting, email, wireless protocols, network communications
Services: Source code reviews and analysis, interviewing technical staff, prior art searching of academic and industrial sources, creating claims charts, drafting expert reports, developing infringement and (in)validity theories, rebutting opposing experts, assisting counsel in depositions, preparing demonstrables for trial, training counsel on technical matters, patent portfolio review

Special Projects

Creator and maintainer of a PROLOG-style logic programming module for Python available at <http://www.multiparadigm-python.org>.

Development of PLAYGROUND, a pedagogical model for network security instruction. **Public Release 2015.**