

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2025-01201
Patent 8,904,194

EXHIBIT 2031

DECLARATION OF AVIEL D. RUBIN, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS	1
III. BASES OF OPINIONS	7
IV. APPLICABLE LEGAL STANDARDS.....	9
A. Level Of Ordinary Skill In The Art.....	9
B. My Understanding Of Legal Standards.....	11
V. CLAIMS-AT-ISSUE (CLAIMS 1-20)	13
VI. Background	14
A. Overview Of The '194 Patent And The Challenged Claims.	14
B. Overview Of Dickinson.....	18
C. Overview of Hardjono.	24
VII. OPINIONS.....	26
A. “Receiving, At The Electronic Computing System/Primary Interface, A Request To Retrieve The Data Set”	26
B. “Generating . . . A Plurality Of Shares”	31
a. “Performing A Cryptographic Operation.”	32
b. “Distributing The Data Set In The Plurality Of Shares Such That The Data Set Can Be Reconstructed Using Any Subset Of The Shares That Includes At Least A Minimum Number Less Than All Of Shares.”.....	37
C. Motivation To Combine Dickinson And Hardjono To Achieve “Sending The Data Set Responsive To The Request”	41
VIII. CONCLUSION	49

I. INTRODUCTION

1. My name is Aviel D. Rubin. I have been retained as an expert witness to provide my independent opinion in regard to the matters at issue in *inter partes* review of U.S. Patent No. 8,904,194 (“the ’194 Patent”) in IPR2025-01201. I have been retained by Security First Innovations, LLC (“SFI”), the Patent Owner in the above proceedings. Petitioner is International Business Machines Corporation (“IBM” or “Petitioner”).

2. I am being compensated \$925 per hour for my time spent working in connection with this case. My compensation is in no way related to the outcome of this litigation. If called as a witness, I would testify as to the statements and opinions contained in this report.

3. I am not a legal expert and offer no opinions on the law. However, I have been informed by counsel of the various legal standards that apply, and I have applied those standards in arriving at my conclusions.

II. QUALIFICATIONS

4. I have more than 30 years of experience in the fields of computer science and applied cryptography. My professional career has been dedicated to issues relating to software, networks, and computer systems more generally.

5. I received a Bachelor of Science in Computer Science with Honors from the University of Michigan in 1989, a Master of Science in Computer Science

and Engineering from the University of Michigan in 1991, and a Ph.D. in Computer Science and Engineering from the University of Michigan in 1994. My Ph.D. dissertation was titled “Nonmonotonic Cryptographic Protocols” and concerned authentication in long-running network operations.

6. I am a Professor Emeritus in Computer Science at Johns Hopkins University (the “University”). I joined the Computer Science faculty at the University in 2003 and was promoted to full professor with tenure in April 2004. As a member of the faculty, I perform research, teach graduate and undergraduate courses in computer science and related subjects, advise undergraduate and Masters students, and supervise the research of Ph.D. candidates and other students. I have taught courses including Networking, Security and Privacy in Computing, Cryptography, and Advanced Topics in Computer Security. In September 2023, I was appointed Professor Emeritus.

7. I also served as the Technical Director of the University’s Information Security Institute (“ISI”). The ISI is the University’s focal point for research and education in information security, assurance, and privacy. The University, through the ISI’s leadership, has been designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and leading experts in the field.

8. I also have significant industry experience. Since 2011, I have served as the founder and chief scientist of Harbor Labs, a software and networking consulting firm specializing in data security and privacy. Previously, from 2005 to 2011, I served as the founder and President of Independent Security Evaluators (“ISE”), a computer security consulting firm. In that capacity, I guided ISE through the qualification process to become an independent testing laboratory for Consumer Union, which produces the Consumer Reports magazine. ISE provided consulting services to various companies on potential security flaws and weaknesses in products and systems. These companies included Fortify Software, Verdasys, and Security First Corp. As an independent testing laboratory for Consumer Union, I managed an annual project where we tested popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years.

9. In addition, I came to the University from AT&T Labs, Secure Systems Research Department, where I spent six years focused on Internet and computer security. Prior to AT&T Labs, I spent two years at Bellcore in its Cryptography and Network Security Research group, also focusing on Internet and computer security issues. I also interned at IBM in 1989. During my time there, I worked on the IBM System/360 family of mainframe computer systems.

10. I am the author or co-author of five books regarding information security issues: *Brave New Ballot*, Random House, 2006; *Firewalls and Internet Security* (second edition), Addison Wesley, 2003; *White-Hat Security Arsenal*, Addison Wesley, 2001; *Peer-to-Peer*, O'Reilly, 2001; and *Web Security Sourcebook*, John Wiley & Sons, 1997.

11. I have received numerous awards for my work and research in the field of computer security, including:

- In 2020, I received the Distinguished Service Award from the Institute of Electrical and Electronics Engineers (“IEEE”) Computer Society Technical Committee on Security and Privacy;
- In 2010, I received a Fulbright Scholarship to serve as a Visiting Professor at Tel Aviv University in Israel;
- In 2009, I received a Google Research Award for my work on securing medical records on smartphones;
- In 2007, I received the Privacy Enhancing Technologies Award for Outstanding Research for my work on a security analysis of a cryptographically enabled RFID device;
- In 2004, I was named Baltimorean of the Year by Baltimore Magazine for my work in safeguarding the election process;

- In 2004, I received the Electronic Frontiers Foundation Pioneer Award; and
- In 2000, I received the Best Paper Award at the 9th USENIX Security Symposium.

12. I serve, or have served, on several technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. In addition, I have been Associate Editor of the IEEE Security and Privacy Magazine and served as Associate Editor of the Association for Computing Machinery's ("ACM") Transactions on Internet Technology. I also served as Associate Editor of the journal Communications of the ACM, and I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I also have served in the past as a member of the Defense Advanced Research Projects Agency's Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, a member of the AT&T Intellectual Property Review Team, Associate Editor of the Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, a member of the board of directors

of the USENIX Association (the leading academic computing systems society), and a member of the editorial board of the Bellcore Security Update Newsletter.

13. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics “Security of Electronic Voting” to Computer Security 2004 Mexico in Mexico City, Mexico, in May 2004; “Electronic Voting” to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington, D.C., in December 2003; “Security Problems on the Web” to the AT&T EUA Customer Conference in March 2000; and “Security on the Internet” to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and another TEDx talk on the same topic in September 2015.

14. I am a named inventor on 10 United States patents, including U.S. Patent Nos. 5,638,446 (“Method for the Secure Distribution of Electronic Files in a Distributed Environment”) and 5,809,140 (“Session Key Distribution Using Smart Cards”).

15. A detailed record of my professional qualifications is set forth in the attached Exhibit A, which is my *curriculum vitae*, including a list of publications, awards, research grants, and professional activities. My *curriculum vitae* also lists the matters in which I have served as an expert.

III. BASES OF OPINIONS

16. In the course of conducting my analysis and forming my opinions, I have reviewed materials including those listed below:

- i. U.S. Patent No. 8,904,194 (Ex. 1001) (“the ’194 Patent” or “’194”);
- ii. The prosecution history of the ’194 Patent (Ex. 1006);
- iii. The Declaration signed by Dr. Erez Zadok, Ph.D. in IPR2025-01201 (Ex. 1002) (the “Zadok Declaration”);
- iv. The Curriculum Vitae of Dr. Erez Zadok (Ex. 1016);
- v. The Petition by IBM in IPR2025-01201;
- vi. PCT Patent Application Publication No. 01/022322 (“Dickinson”) (Ex. 1003);
- vii. U.S. Patent No. 6,363,481 (“Hardjono”) (Ex. 1004);
- viii. Claudia Canali *et al.*, *Performance Comparison of Distributed Architectures for Content Adaptation and Delivery of Web Resources*, 25 IEEE Int’l Conf. on Distributed Comput. Sys. Workshops 331 (2005) (“Canali”) (Ex. 1005);
- ix. File History of U.S. Patent Application Serial No. 11/258,839 (“’839 App. File History”) (Ex. 1007);
- x. U.S. Provisional Application Serial No. 60/622,146 (“Provisional Application No. 60/622,146”) (Ex. 1009);

- xi. U.S. Provisional Application Serial No. 60/718,185 (“Provisional Application No. 60/718,185”) (Ex. 1010);
- xii. Microsoft Computer Dictionary (Ex. 1011);
- xiii. Bruce Schneier, *Applied Cryptography*, 2nd ed., 1996, excerpts (“Schneier”) (Ex. 1012);
- xiv. Highlighted Comparison Between Dickinson and the ’194 Patent (Ex. 1013);
- xv. Yitzhak Birk, “Random RAIDs with Selective Exploitation of Redundancy for High Performance Video Servers,” *IEEE* 1997 (“Birk”) (Ex. 1014);
- xvi. U.S. Patent Publication No. 2003/0016596A1 (“Chiquoine”) (Ex. 1016);
- xvii. John Kubiawicz, et al., “OceanStore: An Architecture for Global-Scale Persistent Storage,” *ACM* 2000 (“Kubiawicz”) (Ex. 1017);
- xviii. U.S. Patent Publication No. 2001/0034795 (“Moulton”) (Ex. 1018);
- xix. U.S. Patent Publication No. 2003/0046551 (“Brennan”) (Ex. 1019);
- xx. U.S. Patent Publication No. US2002/0049655 (“Bennet”) (Ex. 1020);
- xxi. *Google, LLC v. Security First Innovations, LLC*, IPR2024-00212, Exhibit 1043 (Patent Owner’s Proposed Claim Constructions In

Security First Innovations, LLC v. Google, LLC, No. 2:23-cv-00097
(E.D. Va.) (“PO’s Google Litigation Construction”) (Ex. 1021);

xxii. The exhibits and other documents cited herein.

IV. APPLICABLE LEGAL STANDARDS

A. Level Of Ordinary Skill In The Art

17. My opinions in this declaration are based on the understandings of a person of ordinary skill in the art, which I understand is sometimes referred to as an “ordinary artisan” or by the acronyms “POSITA” or “PHOSITA,” as of the time of the invention, which I understand is here assumed to be the effective filing date (October 25, 2004) of the provisional application from which the ’194 patent issued. I understand that the person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. By “relevant,” I mean relevant to the challenged claims of the ’194 Patent.

18. I understand that factual indicators of the level of ordinary skill in the art include the various prior art approaches employed, the types of problems encountered in the art, the rapidity with which innovations are made, the sophistication of the technology involved, and the educational background of those actively working in the field. I understand that, in assessing the level of skill of a person of ordinary skill in the art, one should consider the type of problems encountered in the art, the prior solutions to those problems found in the prior art

references, the rapidity with which innovations are made, the sophistication of the technology, the level of education of active workers in the field, and my own experience working with those of skill in the art at the time of the invention.

19. In this case, Dr. Zadok has asserted in his declaration that a person of ordinary skill in the art as of the time of the '194 Patent would have had:

a Bachelor's degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent field, and about 2-3 years of experience in the fields of data storage and security. Less professional experience can be substituted by additional education, and vice versa.

Ex. 1002 [Zadok-Decl.], ¶ 158.

20. For the purposes of this declaration, I accept Dr. Zadok's proposed qualifications of a POSITA. I reserve the right to revisit the issue should the Petition be instituted.

21. As further discussed below, my opinions as stated in this declaration are valid even if the Board adopts a slightly different level of ordinary skill in the art. For example, as will be discussed throughout my report, even a person with the level of knowledge or experience described by Dr. Zadok or adopted by the Board would not have a reasonable expectation of success in implementing certain aspects of the proposed combination as of the priority date of the '194 Patent.

B. My Understanding Of Legal Standards

22. When considering the '194 Patent and stating my opinions, I rely on the following legal standards as described to me by the attorneys for SFI.

23. I understand that a patent claim is unpatentable if the claimed invention was anticipated by a prior art reference or would have been obvious to a person of ordinary skill in the art at the time of the purported invention.

24. I understand that anticipation requires that every limitation of the claim at issue be disclosed, either expressly or under principles of inherency, in a single prior art reference.

25. I understand that inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient. Instead, it must be proved that the claim limitation not expressly found in the reference necessarily follows from what is found there.

26. I understand that an obviousness analysis involves comparing a claim to the prior art to determine whether the claimed invention would have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art and in light of the general knowledge in the art as a whole. I also understand that obviousness is ultimately a legal conclusion based on underlying facts of four general types, all of which must be considered: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences

between the claimed invention and the prior art; and (4) any objective indicia of non-obviousness, including any praise of the invention.

27. I also understand that obviousness may be established under certain circumstances by combining or modifying the teachings of the prior art. Specific teachings, suggestions, or motivations to combine any first prior art reference with a second prior art reference can be explicit or implicit, but must have existed before the date of purported invention. I understand that prior art references themselves may be one source of a specific teaching or suggestion to combine features of the prior art, but that such suggestions or motivations to combine art may come from the knowledge that a person of ordinary skill in the art would have had.

28. I understand that a reference may be relied upon for all that it teaches, including uses beyond its primary purpose, but also including teachings that lead away from the invention. I understand that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, although the mere disclosure of alternative designs does not teach away.

29. I further understand that whether there is a reasonable expectation of success in combining references in a particular way is also relevant to the analysis.

30. I understand that it is improper to use hindsight to combine references or elements of references to reconstruct the invention using the claims as a guide. My analysis of the prior art is made from the perspective of a person of ordinary skill in the art at the time of the invention.

31. I am not offering any legal opinions in this declaration nor am I qualified to do so. I only consider such legal standards in framing my opinions and conclusions as well as placing assertions made by Petitioner in the Petition into the proper context. Additionally, from a subject matter perspective, I understand that the petitioner always has the burden of persuasion regarding a challenge of patentability of an invention under an inter partes review.

V. CLAIMS-AT-ISSUE (CLAIMS 1-20)

32. I understand that Petitioner has challenged claims 1-20 of the '194 patent based on two grounds:

- Ground I: Claims 1-20 based on obviousness over Dickinson and Hardjono;
- Ground II: Claims 2, 8, 15 based on obviousness over Dickinson, Hardjono, and Moulton.

33. I understand that the challenged independent claims are Claims 1, 7, and 14. At this preliminary stage, my opinions are focused on the independent

claims and, therefore, on Ground I. I reserve the right to revisit both Grounds and offer additional opinions should the Petition be instituted.

VI. BACKGROUND

A. Overview Of The '194 Patent And The Challenged Claims.

34. The '194 Patent is titled "Secure Data Parser Method And System" and is used in "any suitable system for securely storing and communicating data." Ex. 1001 ['194], Title, Abstract.

35. The '194 Patent's inventions and related disclosure generally concern securing "any data set" by encrypting the data set and splitting the encrypted data set into shares using "cryptographic splitting" or a "cryptosplit" process." *See, e.g.,* Ex. 1001 ['194], 52:12-13 (teaching that the data set to be secured is "encrypt[ed], cryptographically split, dispersed and securely stored in multiple locations"). Following encryption of the data set, a cryptosplit "partitions the data [set] into N number of shares" based on "any size unit of data," including "bits, bytes, kilobytes, megabytes or larger units." *Id.*, 52:40-44. The units are "distributed (either randomly or by a predetermined set of values)" into the N shares. *Id.*, 52:51-53. This means that each share "can be viewed as a sequence of these units." *Id.*, 52:46-47.

36. The '194 Patent also discloses “redundancy functionality,” which appends redundancy information to each share so that the data set may be recreated from fewer than all of the shares. *Id.*, 72:36-39.

37. The '194 Patent also discloses storing the shares on a plurality of different storage devices, as well as the ability to retrieve the shares of the data set from storage, reconstruct the data set by reversing the storage process, and return the reconstructed data set to the user. *See id.*, cls 1, 7, 14. To facilitate an efficient share retrieval process, the '194 Patent teaches that when a user requests stored data, the system should (i) identify a “set” of fastest-responding storage devices that contain the minimum number of shares necessary to retrieve the data; (ii) reconstruct the data set; and (iii) send the reconstructed data set to the user. *Id.*

38. The overall system/process used by the secure parser is shown in Figures 31 and 32 (below). Figure 31 shows a block diagram of a process used to “write” a data set “to a storage device.” *Id.*, 70:43-45. At 3100, the user selects the data to be stored, and the Secure Data Parser Core is called. *Id.*, 70:46-48. The Secure Data Parser Core “parses and splits” the data set, adds redundancy information, and places the shares in Split Data Buffers 3010. *Id.*, 70:54-57; *see also id.*, 69:49-52. The shares are then distributed to different locations for storage by module 3014. Figure 32 shows the reconstruction of the data set when it is “read” from a “storage device.” *Id.*, 70:64-66. At 3200, the data to be restored is

identified, and Secure Data Parser Core 3000 is called. The Secure Data Parser Core reverses the process of Figure 31: The shares are collected from storage locations, redundant information is removed (or fewer than all of the shares are used), and the data set is assembled from the shares and transmitted to the requester. *Id.*, 71:1-15.

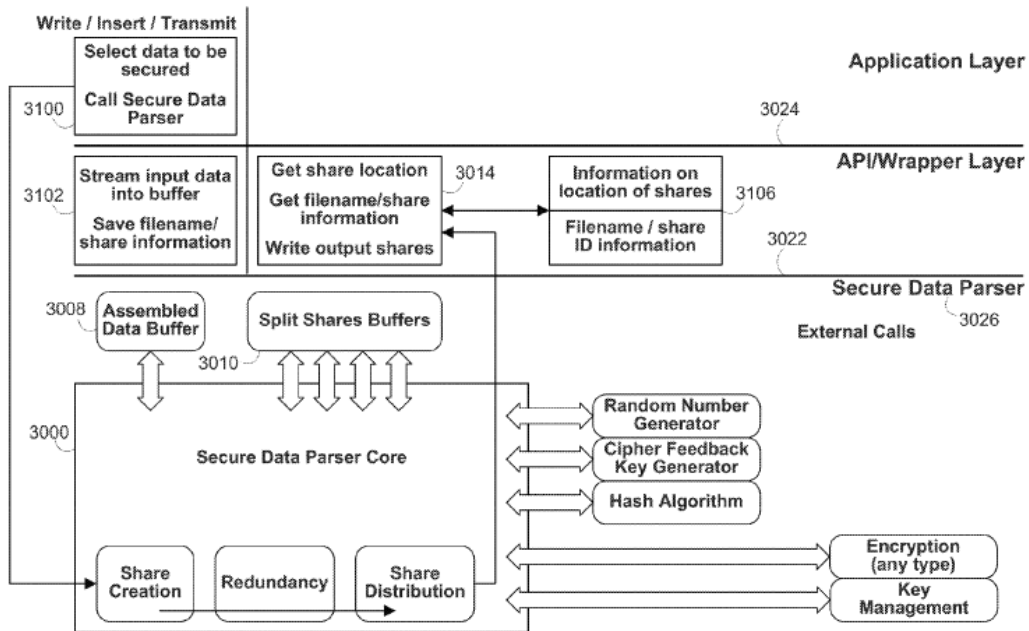


FIG. 31

Ex. 1001 [’194], Fig. 31.

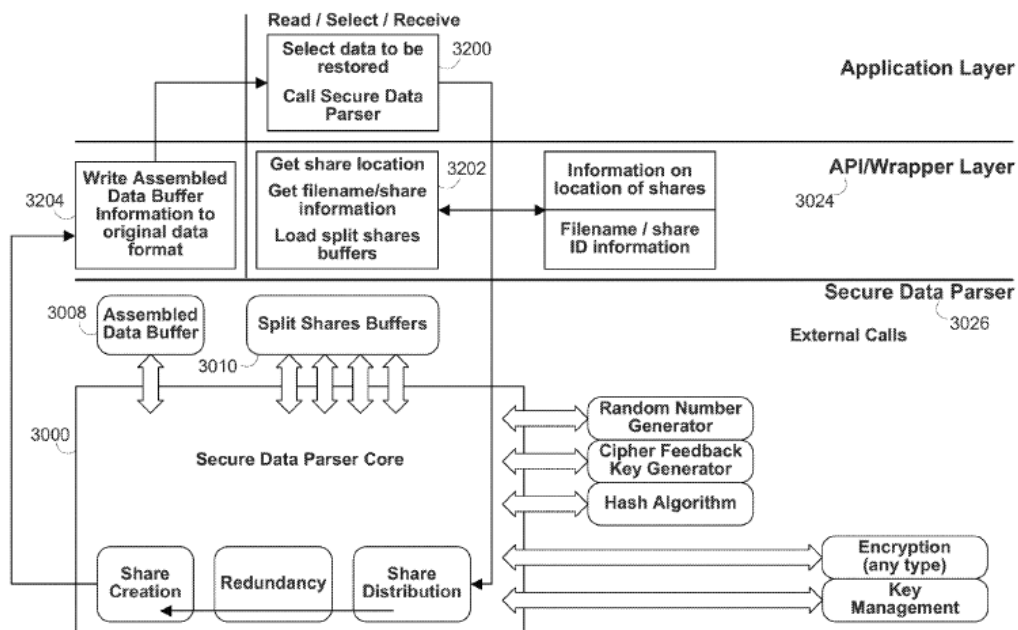


FIG. 32

Id., Fig. 32.

39. The independent claims of the '194 Patent teach the above-described process. They require encrypting a data set by “performing a cryptographic operation;” parsing the encrypted data set into shares “such that the data set can be reconstructed using . . . less than all of the shares;” and storing the shares on a plurality of storage devices. *Id.*, cls. 1, 7, 14. Then, on receiving a “request to retrieve the data set,” identifying “a set of fastest-responding storage devices”; “retrieving from the set . . . the minimum number of shares” needed to reconstruct the data set; “reconstructing the data set from the minimum number of shares”; and finally “sending the dataset” in response to the request. *Id.*

B. Overview Of Dickinson.

40. Dickinson is titled “Electronic Commerce With Cryptographic Authentication” and relates to a “method for facilitating an authentication related to an electronic transaction between a first and a second user.” Ex. 1003 [Dickinson], Title, Abstract.

41. Dickinson addresses a “need . . . for [an] authentication system[] which provide[s] security for electronic transactions” between a vender and user that is “sufficient for the needs of a vendor without unnecessary inconvenience to the user.” *See id.*, 2:8-11. Dickinson discloses a secure server or “trust engine” that stores “cryptographic keys and user authentication data.” *Id.* This “authentication data,” as envisaged in Dickinson, could be an “identification number, one or more biometrics, [or] a series of questions” about a user’s “place of birth, address, anniversary, . . . mother’s maiden name, favorite ice cream, or the like”). *Id.*, 10:20-29. Dickinson’s trust engine includes an “authentication engine” that compares the user’s “enrollment authentication data,” stored within Dickinson’s secure server, with “current authentication data” provided by the user at the time of a transaction. *Id.*, 3:3-13. If the user’s “current authentication data” matches their “enrollment authentication data,” Dickinson will confirm for the vendor that the user is authentic. *Id.*, 5:24-25, 55:11-16. A positive comparison authenticating the user allows him or her to carry out a number of cryptographic

operations, including “authentication, authorization, digital signing and generations, storage and retrieval of certificates,” etc. *Id.*, 2:8-14.

42. Unlike the '194 Patent, Dickinson does not disclose either encryption or storage of a data set (other than the enrollment authentication data for purposes of comparison) or returning a previously stored data set to the user at the user or vendor's request. The enrollment authentication data is never provided to the user or vendor; in fact, once stored, it never leaves Dickinson's system—specifically, Dickinson's “Trust Engine 110.”

43. As Dickinson explains, Trust Engine 110 comprises a “transaction engine 205,” a “depository 210,” “an authentication engine 215”, and a cryptographic engine 220. *Id.*, 13:5-7. The transaction engine 205 provides the sole external communication link with the Trust Engine 110. It provides front end security by “receiv[ing] incoming data,” including authentication requests, over the Communication Link and routing that data to the appropriate module of the trust engine. *Id.*, 13:25-28. Depository 210 comprises one or more storage facilities for storing private encryption keys (corresponding to users and vendors) and enrollment authentication data, none of which ever leaves Trust Engine 110. *Id.*, 14:17-19, 28:30-31 (“Moreover, the authentication result transmitted to the vendor does not include the sensitive data.”). Authentication engine 215 “comprises a data comparator” that compares authentication data from transaction engine 205

with enrollment authentication data from depository 210, to verify a user's identity. *Id.*, 15:4-12. Finally, the cryptographic engine 220 is "configured to advantageously provide conventional cryptographic functions" to a user whose identity has been verified. *Id.*, 15:21-22. Dickinson suggests that these various functions could include "digital signing, encryption, decryption, hash creation, key generation,[] key destruction," "logging into a portal," or "unlocking a password vault," (*id.*, 55:33-56:9), but it does not teach methods to implement any of these cryptographic functions.¹

¹ For example, Dickinson notes that the cryptographic engine 220 may generate public and private encryption keys on behalf of a user of the Trust Engine 110, such that "the private cryptographic keys are not available outside of the trust engine." *Id.*, 15:20-30.

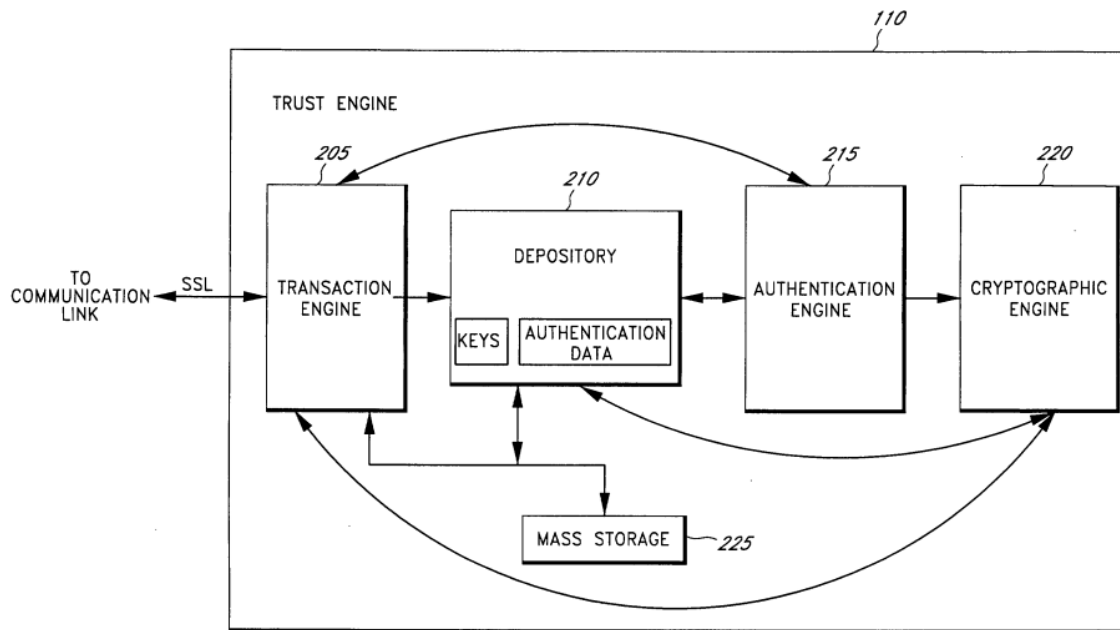


FIG. 2

Id., Fig. 2.

44. Dickinson’s trust engine works by receiving an authentication request from a vendor, which prompts the system to forward a transaction identifier (“TID”) and the user’s “enrollment authentication data” to its “authentication engine.” Ex. 1003 [Dickinson], 55:3-9. Next, Dickinson “quer[ies] the user for current authentication data and the TID,” which it also forwards to the “authentication engine.” *Id.*, 55:10-12. After comparing the “enrollment authentication data” and “current authentication data,” the “authentication engine” outputs a result that indicates whether the data match. *Id.*, 45:23-25, 55:15-16. This verifies the identity of the user and thus secures the transaction.

45. Central to Dickinson, however, is that the enrollment authentication data stored in depository 210 never leaves the trust engine. *See id.*, 28:30-31. This ensures that the private encryption keys and enrollment authentication data is provided “in an environment where they are not lost, stolen or compromised, thereby advantageously avoiding a need to continually reissue and manage new keys and authentication data.” *Id.*, 2:19-21. To that end, and contrary to Petitioner’s characterization, Dickinson does not receive requests to “write or store a data set,” nor to retrieve or send data stored in depository 210 in response to such a request. *See Pet.*, 15. Rather, Dickinson requires only a request for authentication and the “authentication data” as input, and it returns as output (1) a binary “YES/NO . . . result” or (2) the result of a cryptographic operation (*i.e.*, a digital signature or certificate) if the user’s identify is verified. Ex. 1003 [Dickinson], 28:20-24, 31:17-21.

46. Dickinson also fails to disclose distributing a data set into “shares.” In fact, Dickinson uses the term “share” only three times in 54 pages of text and never to refer to a piece of a data set. *See generally id.* As explained below, there simply is no disclosure in Dickinson that partitions a data set into N shares by distributing units of that data set (*i.e.*, its bits, bytes, kilobytes, etc.) either randomly or by a “predetermined set of values” such that each share “can be viewed as a sequence of these units.” *See Ex. 1001 [’194], 52:45-48.*

47. Dickinson shares three inventors of the '194 Patent: Orsini, O'Hare and Davenport. Petitioner claims that because Figures 1-20—and thus much of the discussions associated with those figures in the '194 Patent—are the same as those in Dickinson, the reference “provides invalidating disclosures for most of the '194 Patent’s claim limitations.” Pet., 12. That is simply wrong. Immediately *following* the portion of its specification that is also in Dickinson, the '194 Patent states that “in a separate embodiment, the present invention comprises a complete system,” called the secure data parser, that operates “on any data set.” Ex. 1001 ['194], 51:55-57. The limitations of the inventions claimed in the '194 Patent are disclosed and enabled in the subsequent 15 figures and 25 columns of text that are not in Dickinson. These include “generating . . . a plurality of shares by “performing a cryptographic operation on a dataset and distributing the *data set* in the plurality of shares”; “receiving . . . a request to retrieve the data set”; and “sending the data set responsive to the request” to the requestor. *See id.*, 75:24-48.

48. I note that the Examiner considered a substantially similar Dickinson reference during prosecution of the '194 patent. Ex. 1006 [Prosecution-History], 217. Indeed, that Dickinson reference is listed on the face of the '194 Patent. Ex. 1001 ['194], 4.

C. Overview of Hardjono.

49. Hardjono is titled “Method And Apparatus For Secure Data Storage Using Distributed Databases.” Ex. 1004 [Hardjono], Title; *see also* Abstract. I note that the Examiner considered Hardjono during prosecution of the ’194 Patent. Ex. 1006 [Prosecution-History] 681; Ex. 1001 [’194], 2.

50. Hardjono addresses the “vulnerab[ility]” of data storage systems “comprising a single [encryption] key” that, if compromised, would allow “an unauthorized individual [to] access the data” (Ex. 1004 [Hardjono], 1:23-29) which is a different concern than Dickinson’s. To address this concern, Hardjono teaches “a method and apparatus for data storage using distributed databases.” This includes generating a “plurality of shares” from an input data set such that “at least a subset” of the shares is required to recover the original data, then distributing the “plurality of shares . . . to a plurality of distributed databases.” *Id.*, 1:47-53.

51. Upon receipt of an input data block, Hardjono generates a password to associate with the data block “for use in later re-creation of the block of data.” *Id.*, 9:48-51. Hardjono then encrypts the data block with a key, generates a “first plurality of shares based on the block of data,” and “distribut[es] the first plurality of shares to a plurality of distributed databases.” *Id.*, 9:51-59. Next, Hardjono generates a “second plurality of shares based on the encryption key” and

“distribut[es] the second plurality of shares to the plurality of distributed databases.” *Id.*, 9:59-65.

52. When Hardjono “receives a request to retrieve the block of data,” the system confirms that the request provided the correct password, accesses the required “subset of the plurality of databases to retrieve a second plurality of shares,” then reconstructs the input data block “using the second plurality of shares.” *Id.*, 10:7-14.

53. Hardjono also teaches an “apparatus” to perform this method, comprising several connected modules that perform the various steps and communicate with other modules in the system. *See Id.*, 10:23-54. These modules include (i) “a verification controller” that establishes the password, (ii) either a database or storage controller that stores the password, (iii) “a storage controller” that encrypts the data, (iv) “a share generator” that generates the first and second pluralities of shares, and (v) “a share distributor” that places the shares into the distributed databases. *Id.*, 10:23-54.

54. I note that Hardjono does not teach “generating ... a plurality of shares by performing a cryptographic operation” (Ex. 1001 [’194], cls. 1, 7, 14) as Hardjono merely teaches that shares are “create[ed]” or “generated.” *See, e.g.*, Ex. 1004 [Hardjono], 3:29-31, 3:39-40.

VII. OPINIONS

A. “Receiving, At The Electronic Computing System/Primary Interface, A Request To Retrieve The Data Set”

55. The claims require:

Limitation 1[C] “receiving, at the electronic computing system, request to retrieve the data set;”

Limitation 7[B-3] “receive, via the primary interface, a request to retrieve the data set;”

Limitation 14[D] “receive a request to retrieve the data set;”

56. I understand that Petitioner argues that Dickinson alone “discloses” this limitation for each of the independent claims. Pet., 44 (“Dickinson discloses 1[C].”), 60 (“Dickinson discloses [7B-3].”), 71 (“Dickinson discloses [14D] for the reasons provided in . . . [Ground I, 7B-3].”). More specifically, Petitioner argues that Dickinson discloses these limitations because “the vendor system 120 . . . forwards . . . the authentication request to the trust engine 110,” and that “the transaction engine 205 [of trust engine 110] receives the [communication authentication request].” *E.g.*, Pet., 45 (quoting Ex. 1003 [Dickinson], 28:6-14). I disagree.

57. In the ’194 Patent, the “request to retrieve the data set” is a call to restore an identified data set so that it may be sent back to the requester in its original format. This request process can be seen illustrated in Figure 32, below:

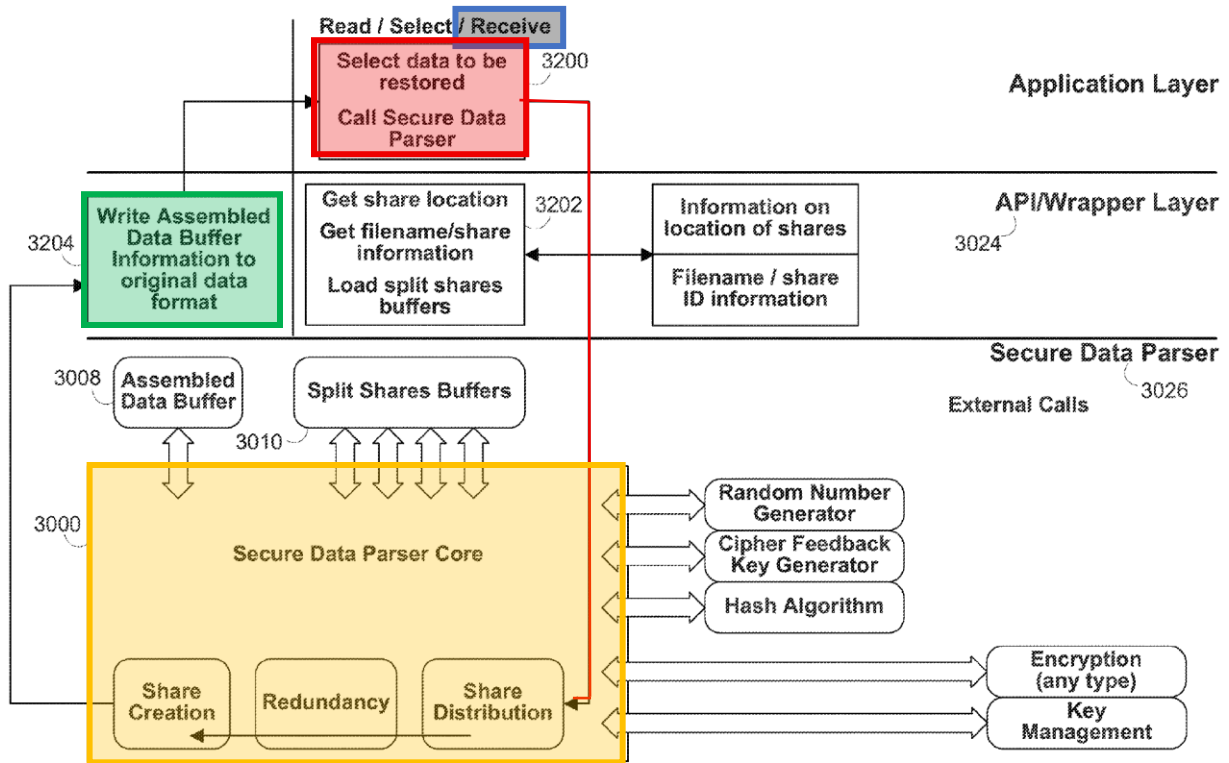


FIG. 32

Ex. 1001 [’194], Fig. 32 (annotated). The ’194 Patent describes that a “request” to “read” an “identified” data set from a storage device may be “receive[d]” by the Secure Data Parser Core. *Id.*, 70:64-67. As can be seen in Figure 32 above, the Secure Data Parser Core, corresponding to the electronic computing system (or primary interface), “receives” a request from an external system which causes the Secure Data Parser Core to **reassemble the data** so that it is **converted to its “original format”** and may be sent back to the requester. *Id.*, 70:64-71:14.

58. In my opinion, Dickinson fails to disclose this limitation because its “authentication request” is not the “request to retrieve a data set” disclosed and claimed in the ’194 Patent. Dickinson’s authentication requests are not directed to

retrieving or restoring an identified data set. Rather, Dickinson’s requests are directed to authenticating a user, *i.e.*, by confirming that the current authentication data matches the enrollment authentication data. *See, e.g.*, Ex. 1003 [Dickinson], 27:15-16 (“the authentication process 1000 includes gathering current authentication data from a user and **comparing** that to the enrollment authentication data of the user.”). The “authentication request” in Dickinson that Petitioner relies upon is simply a request to compare information and provide a response based on the result of the comparison—*i.e.*, whether or not the user is verified. As Dickinson explains, “authentication is the process of proving that a user is who he says he is. Generally, authentication requires demonstrating some fact to an authentication authority.” *Id.*, 37:24-29. Notably, Dickinson’s authentication process does not need the vendor to receive the enrollment authentication data.

59. I note that Petitioner only relies upon Dickinson’s “authentication request”—*i.e.*, a request to determine whether the user “is who he says he is” (*Id.*, 37:24)—and not a request to retrieve a particular data set for the user or vendor. *Pet.*, 49. Again, however, an authentication request is not a request to retrieve a data set. Indeed, Dickinson expressly teaches that the response to an authentication request “does not include” the underlying enrollment authentication data—the only “data set” stored by the secure data parser. Ex. 1003 [Dickinson],

28:30-31 (“Moreover, the authentication result transmitted to the vendor does not include the sensitive data, and the user may not even know whether he or she produced valid authentication data.”).

60. What is more, the distinction between an authentication request and a request to “retrieve the data set” is an important one that is made expressly clear in the ’194 Patent itself. The ’194 Patent’s specification specifically distinguishes “requests to retrieve the data set” as discussed, *e.g.*, in connection with Figure 32 (*see* Ex. 1001 [’194], 70:65-71:15), from “authentication requests.” *See, e.g., id.*, 26:24-27:52; *see also id.*, 36:21-22 (“authentication is the process of proving that a user is who he says he is”).

61. Petitioner also seems to rely on Dickinson’s disclosure that, in response to receiving an authentication request, the transaction engine of the trust engine generates a “request for the user’s enrollment authentication data to be assembled.” Pet., 45. In my opinion, this too fails because that request in Dickinson is not “receiv[ed]” at “the electronic computing system” or “the primary interface,” as required by the ’194 Patent’s independent claims. *See* Ex. 1001 [’194], cls. 1, 7, 14. Petitioner identifies Dickinson’s trust engine as the “electronic computing system” and the “primary interface.” *See, e.g.,* Pet., 35 (“A POSITA would have understood that the trust engine is an example of an electronic computing system.”). But the trust engine does not *receive* a “request

for the user’s enrollment authentication data to be assembled”—it *generates* it.

Dickinson makes clear that it is the transaction engine that generates the “request for the user’s enrollment authentication data.” Ex. 1003 [Dickinson], 28:9-11.

And the *transaction engine* is a module of—*i.e.*, inside of—the *trust engine*:

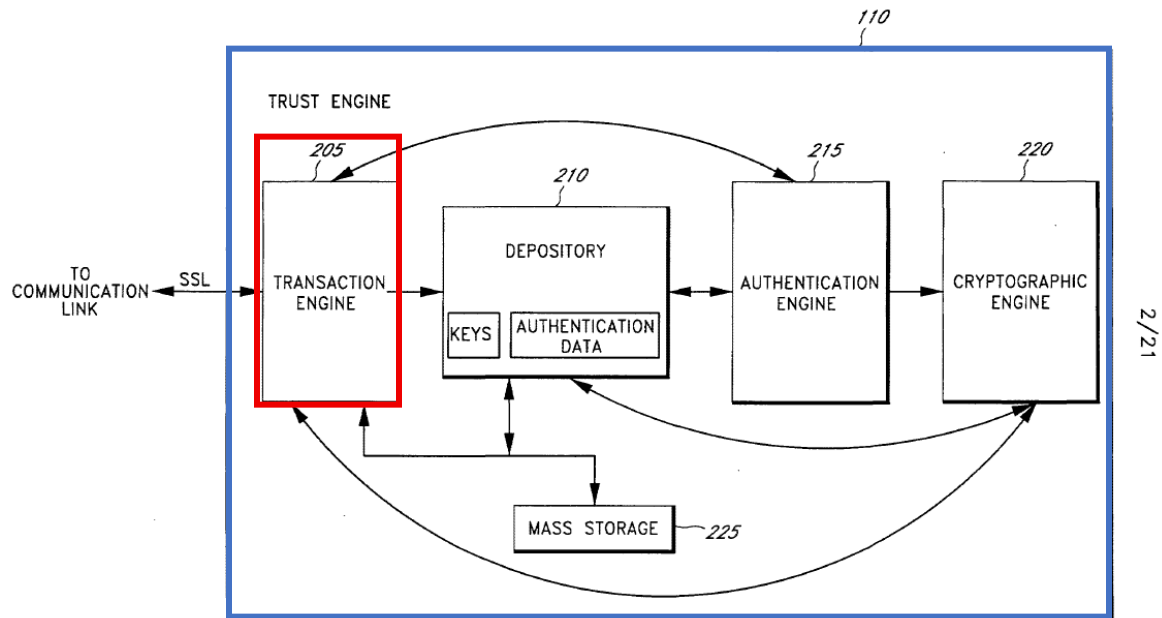


FIG. 2

Id., Fig. 2 (annotated); 13:6-8 (“trust engine 110 includes a transaction engine 205, a depository 210, an authentication engine 215, and a cryptographic engine 220.”).

62. I see no explanation from Petitioner for how Dickinson’s trust engine “receives” a request it generates internally. Certainly, the ’194 Patent does not suggest the electronic computing system would “receive” an internally generated request, confirming a prototypical receipt comes over a network. *See* Ex. 1001 [’194], 70:64-67 (disclosing that a request can be “receive[d] (e.g., from a

network)"). In this, the '194 Patent's usage accords with the common understanding of "receive." Ex. 2032 [Microsoft-Computer-Dictionary], 442 ("receive *vb.* To accept data from an *external* communications system"); Ex. 2033 [Essential-American-English-Dictionary], ("to get something that *someone* has given or sent to *you.*").

63. Thus, in my opinion, Petitioner has failed to show that the authentication requests disclosed in Dickinson constitute a "request to retrieve the data set" at an "electronic computing system" or "primary interface" as required by the independent claims of the '194 Patent.

B. "Generating . . . A Plurality Of Shares"

64. The claims require:

Limitation 1[A-1] "generating, using an electronic computing system that includes processing circuitry, a plurality of shares by performing a cryptographic operation on a data set and"

Limitation 1[A-2] "distributing the data set in the plurality of shares such that the data set can be reconstructed using any subset of the shares that includes at least a minimum number less than all of shares;"

Limitation 7[B-1] "generate a plurality of shares by performing a cryptographic operation on a data set and distributing the data set in the plurality of shares such that the data set can be reconstructed using any subset of the shares that includes at least a minimum number less than

all of the shares and such that the data set cannot be reconstructed using any subset of the shares that includes fewer than the minimum number of the shares;”

Limitation 14[B] “generate a plurality of shares by performing a cryptographic operation on the data set and distributing the data set in the plurality of shares such that the data set can be reconstructed using any subset of the shares that includes at least a minimum number less than all of the shares and such that the data set cannot be reconstructed using any subset of the shares that includes fewer than the minimum number of the shares;”

65. I understand that Petitioner argues that Dickinson alone “discloses” these limitations. Pet., 35-40 (“Dickinson discloses” limitation 1[A-1]), 40-43 (“Dickinson discloses” limitation 1[A-2]), 59 (“Dickinson discloses [7B-1].”), 71 (“Dickinson discloses [14B]”).

66. I do not believe Petitioner and Dr. Zadok have demonstrated that Dickinson “discloses” either “performing a cryptographic operation” in creating the shares or “distributing the data set” into the shares.

a. “Performing A Cryptographic Operation.”

67. To reiterate, the ’194 requires “generating . . . a plurality of shares” by first “performing a cryptographic operation on a data set.” Ex. 1001 [’194] cls. 1[A], 7[B], 14[B].

68. Per the '194 Patent, “cryptography,” in general, refers to “protecting data by transforming, or encrypting, it into an unreadable format” such that “[o]nly those who possess the key(s) to the encryption can decrypt the data into a useable format.” Ex. 1001 [’194], 1:38-41. I note that the ’194 Patent also describes that “[i]ncluded among [the ’194’s cryptographic] functions may be requests associated with performing various cryptographic operations, such as encrypting a document with a particular key[.]” *Id.*, 50:58-61. From this, in my opinion, a POSITA would have understood “cryptographic operation” as used in the ’194 Patent to mean operations that require key encryption, “such as encrypting a document with a particular key.” *Id.*

69. In accord, the ’194 Patent discloses several embodiments in which shares are generated by first encrypting the data set and then distributing the data set into shares. For example, the ’194 Patent discloses an embodiment in which “encryption may occur prior to the splitting of the data set by the splitting module or secure data parser.” Ex. 1001 [’194], 52:29-31; *see also id.*, 52:12-13 (disclosing embodiment in which the data set is “encrypt[ed], cryptographically split, dispersed and securely stored in multiple locations”), 71:32-33 (“In one suitable approach, original data 3306 may be encrypted prior to parsing, splitting or both.”); Figs. 21-24; Figs. 31-32 (disclosing “Encryption—Any Type” as a capability of the Secure Data Parser Core).

70. I note that Petitioner points to three purported teachings in Dickinson to support its contention that Dickinson alone “discloses” “performing a cryptographic operation.” In my opinion, none of these purported teachings discloses “performing a cryptographic operation.”

71. First, Petitioner argues:

Dickinson Figure 5 illustrates that “[t]he data splitting module 520 advantageously comprises a software, hardware, or combination module having the ability to mathematically operate on various data so as to ... *split the data* into *portions*.” EX1003, 18:20–28.

Pet., 36-37. I do not see any explanation of how “mathematically operate” teaches a “cryptographic operation.” Indeed, simply disclosing “having the ability to mathematically operate” does not disclose that the portions are rendered undecipherable without a key, or any other cryptographic operation.

72. Second, Petitioner also relies upon Dickinson’s Figure 8:

In another example, Dickinson explains that “the authentication engine 215 and the *cryptographic* engine 220 may advantageously employ their respective data splitting modules [520 and 610, respectively] to *divide sensitive data* into *undecipherable portions*.” EX1003, 19:27–34. Dickinson Figure 8 “illustrates a flowchart of a data splitting process 800 performed by the data splitting module” and shows that “*sensitive data ‘S’* is received by the data splitting module of ... the cryptographic engine 220” and “the data splitting module then

generates *a substantially random number value, or string or set of bits, 'A'.*” EX1003, 20:20–29, FIG. 8. EX1002, ¶249.

Pet., 37-38. Again, I do not see any explanation of how this discloses a “cryptographic operation.” *Id.* Petitioner never establishes that the “substantially random number value, or string or set of bits” are used to perform a cryptographic operation. I do not see any assertion that Petitioner’s combination uses this random number, let alone any explanation of how the proposed combination would use this random number. *Id.* Thus, in my opinion, this purported teaching also fails.

73. Third, Petitioner relies upon Dickinson’s alleged disclosure that ““the trust engine 110 may advantageously perform . . . data encryption and decryption’ as it generates the plurality of shares.” Pet., 38 (quoting Ex. 1003 [Dickinson], 16:8-10). I note that Petitioner’s quotation of Dickinson is misleading because Dickinson does not disclose that “data encryption” is used when the trust engine “generates the plurality of shares.” The passage states in full and with surrounding context:

Although the trust engine 110 is disclosed with reference to its preferred and alternative embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize in the disclosure herein, a wide number of alternatives for the trust engine 110. For example, the trust engine 110, may advantageously perform only authentication, or alternatively only some or all of the cryptographic functions such as

data encryption and decryption. According to such embodiments, one of the authentication engine 215 and the cryptographic engine 220 may advantageously be removed, thereby creating a more straightforward design for the trust engine 110. In addition, the cryptographic engine 220 may also communicate with a certificate authority such that the certificate authority is embodied within the trust engine 110. According to yet another embodiment, the trust engine 110 may advantageously perform authentication and one or more cryptographic functions, such as, for example, digital signing.

Ex. 1003 [Dickinson], 16:6-14. In context, Dickinson makes clear that the trust engine performs “cryptographic functions” in response to an authentication request, not in the process of generating shares. *See, e.g., id.*, 16:13-14 (“trust engine may advantageously perform authentication and one or more cryptographic functions, such as, for example, digital signing.”). Contrary to Petitioner’s misleading claim, the passage Petitioner relies upon is a reference to Dickinson’s disclosure that when a vendor requests a “cryptographic transaction” such as digital signature, the trust engine will “associat[e] a user . . . with one or more [encryption] keys” stored on its server. *Id.*, 3:13-15, 5:28-30. Only after the trust engine completes its authentication method can the associated key be used to perform whichever “cryptographic function” the vendor requested. *Id.*, 3:13-15, 55:33-56:9.

74. Consequently, in my opinion, Petitioner has failed to demonstrate that Dickinson “discloses” “performing a cryptographic operation.”

b. *“Distributing The Data Set In The Plurality Of Shares Such That The Data Set Can Be Reconstructed Using Any Subset Of The Shares That Includes At Least A Minimum Number Less Than All Of Shares.”*

75. Each of the independent claims require “distributing a data set in a plurality of shares such that the data set can be reconstructed using any subset of the shares that includes at least a minimum number less than all of shares.” Ex. 1001 [’194], cls. 1[A-2], 7[B-1], 14[B].

76. I understand that Petitioner alleges that Dickinson alone “discloses” these limitations, relying on Dickinson’s Figure 7, Figure 8, and associated disclosure. Pet., 40-43. For the reasons stated below, I do not believe that Dickinson’s example discloses “*distributing the data set in the plurality of shares, such that the data set can be reconstructed using any subset of shares that includes a minimum number less than all of shares.*”

77. The ’194 Patent discloses “distributing the data set in the plurality of shares” by disclosing a “cryptographic split (cryptosplit)” that “partitions the data” into N shares based on “any size unit of data.” *Id.*, 52:40-43. The cryptosplit process ensures that *the data set is distributed* among the plurality of shares so that each share includes some portion of the data set. The ’194 Patent provides an

example of a cryptosplit distributing a 23-byte data set into four shares, with a data unit size of one byte:

Each byte would be distributed into one of the 4 shares. Assuming a random distribution, a key would be obtained to create a sequence of 23 random numbers (r1, r2, r3 through r23), each with a value between 1 and 4 corresponding to the four shares. Each of the units of data (in this example 23 individual bytes of data) is associated with one of the 23 random numbers corresponding to one of the four shares. The distribution of the bytes of data into the four shares would occur by placing the first byte of the data into share number r1, byte two into share r2, byte three into share r3, through the 23rd byte of data into share r23.

Ex. 1001 [’194], 52:61-53:7.

78. The ’194 Patent extends this example to disclose how the cryptosplitting process can be used to distribute the data set into shares such that the data set can be reconstructed using *any subset of shares* that includes at least a minimum number less than all of the shares. The ’194 Patent refers to this as an “M of N cryptosplit,” in which the data set can be reassembled from any subset M of the total N shares, where M is at least one less than N. Ex. 1001 [’194], 53:16-26. It discloses that, in one embodiment, an M of N cryptosplit is accomplished by storing each unit of data in both a “primary” share and a “backup” share, where the number of primary shares is N and the number of backup shares is M, and M is at

least one less than N. *Id.*, 53:28-39. By extending the example discussed above, the '194 Patent discloses an M of N cryptosplit for distributing a 23-byte data set into four shares, using a data unit size of one byte, such that the data set can be reconstructed from any 3 of the 4 shares:

[A] set of random numbers (also referred to as primary share numbers) from 0 to 3 are generated equal to the number of data units. Then another set of random numbers is generated (also referred to as backup share numbers) from 1 to 3 equal to the number of data units. Each unit of data is then associated with a primary share number and a backup share number. . . . The primary share number is used to determine into which share the data unit is stored. The backup share number is combined with the primary share number to create a third share number [If] primary share number is between 0 and 3, and the backup share number is between 1 and 3 [that] ensures that the third share number [the backup share number] is different from the primary share number.

Id., 53:40-62. In this case, the result is that each of the four shares contains a portion of the data set and each share contains sufficient redundant data such that the data set can be reconstructed from any subset of three shares.

79. Petitioner relies upon Dickinson's Figure 8 for this limitation, alleging that in Dickinson's Figure 8 example, two random numbers, "A" and "C", are generated by the trust engine. Each of those numbers is then combined with the Sensitive Data ("S") (*i.e.*, enrollment authentication data) using the XOR operation

to create new numbers “B” and “D.” *See Pet.*, 41. The A, B, C and D numbers are combined, in an unexplained way, to form the “pairings” AC, AD, BC and BD “such that any two [pairings] provide one of A and B, or, C and D,” sufficient to reconstruct S. *Id.*, 42 (quoting Ex. 1003 [Dickinson], 21:27-28).

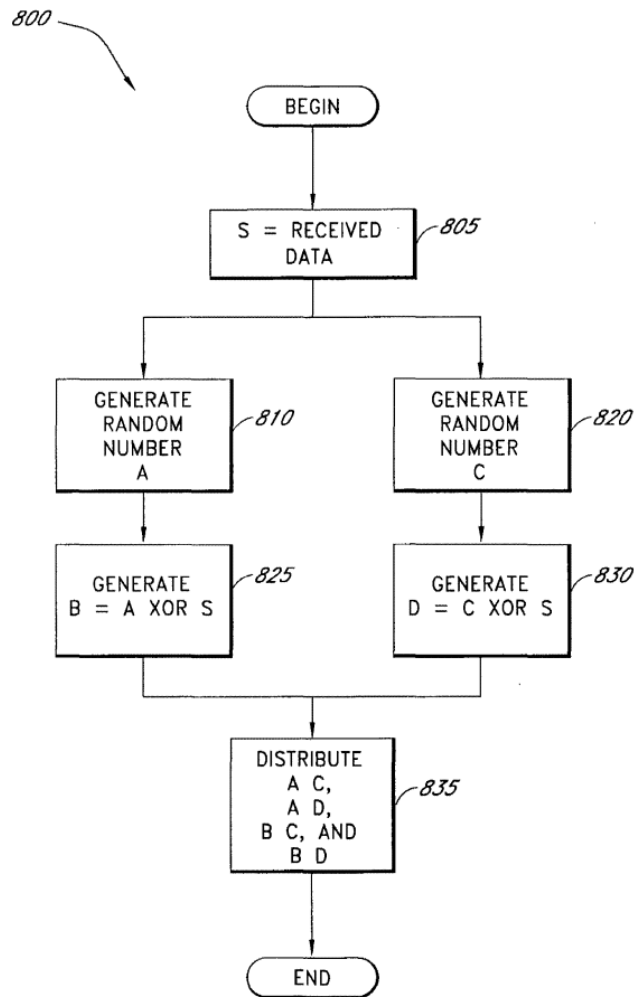


FIG. 8

Ex. 1003 [Dickinson], Fig. 8.

80. In my opinion, while this example may disclose the generation and storage of different numbers (“pairings”) from which S may be recreated, it does not disclose “*distributing*” the “*data set*” S into a plurality of shares in the manner disclosed and claimed in the ’194 Patent. As can be seen above, one of Dickinson’s Figure 8 pairings (AC) contains nothing from S; the AC pairing is simply the two random numbers that were generated by the trust engine. The other pairings (AD, BC, BD) each include at least one copy of S *in its entirety* from B (A XOR S) or D (C XOR S); in fact, the BD includes two copies of S. Whatever may be said about the correspondence between the “pairings” disclosed in Dickinson, and the “shares” required by the ’194 Patent, it is clear that what is “distributed” in the pairings is not *data set* S, as the pairings comprise either none of S or all of it.

81. Thus, in my opinion, Petitioner fails to demonstrate that Dickinson “discloses” distributing a data set into a plurality of shares such that the data set can be reconstructed using any subset of the shares that includes at least a minimum number less than all of the shares.”

C. Motivation To Combine Dickinson And Hardjono To Achieve “Sending The Data Set Responsive To The Request”

82. The claims recite:

Limitation 1[G] “sending the data set responsive to the request.”

Limitation 7[B-6] “send the data set responsive to the request.”

Limitation 14[H] “send the data set responsive to the request.”

83. I note that “the request” in the limitations refers to the earlier “request to retrieve the data set.”

84. I note that Petitioner does not suggest that Dickinson alone discloses this limitation. Pet., 49. Rather, Petitioner relies upon “Dickinson in view of Hardjono” for limitations 1[G] and 7[B-6]. *Id.*, 49, 63. I note that for limitation 14[H], Petitioner appears to contend that “Dickinson discloses [14H]” but relies wholly upon its analysis in connection with limitation 7[B-6]. *Id.*, 72. In connection with limitation 7[B-6], however, Petitioner relies upon the combination with Hardjono. *Id.*, 63. No explanation is given for how Dickinson alone would satisfy the limitation requiring “send[ing] the data set responsive to the request.” In any case, in my opinion, Petitioner and Dr. Zadok have failed to demonstrate that a POSITA would be motivated to combine Dickinson and Hardjono to permit sending the highly sensitive data stored in Dickinson’s trust engine, outside the system.

85. The ’194 Patent discloses that “one aspect of the present invention is to provide a method for securing virtually any type of data from *unauthorized* access or use.” Ex. 1001 [’194], 2:33-35. The method also “comprises reconstituting or re-assembling the secured data into its original form for *authorized* access or use.” *Id.*, 2:46-48. Access to or use of the requested data by an authorized user requires sending the reconstituted data external to the Secure

Data Parser. Likewise, Figure 32 discloses the operation of the secure data parser when it receives a “read” request to obtain data stored in the system. *Id.*, 70:64-71:14. In this example, the secure parser collects the shares, reconstitutes the data set, and sends it on for, *e.g.*, external “communicat[ion] o[ver] a network” to the requester. *Id.*, 70:63.

86. In Dickinson, after a user initiates a transaction with a vendor, the vendor sends an authentication request to the trust engine, which ultimately determines whether the user is authenticated and reports the result back to the vendor or provides a cryptographic function such as providing a digital signature. Ex. 1003 [Dickinson], 28:20-24. This method makes perfect sense; a user attempts to initiate a transaction and the trust engine authenticates the user before proceeding with verifying the transaction or providing the signature.

87. Dickinson does not, however, “send[] the data set responsive to the request” as the claims require. Indeed, Dickinson expressly teaches that the authentication result returned to the vendor in response to the authentication requests does *not* include the sensitive data. *Id.*, 28:30-31 (“Moreover, *the authentication result transmitted to the vendor does not include the sensitive data*, and the user may not even know whether he or she produced valid authentication data.”).

88. I note that Petitioner appears to acknowledge Dickinson’s deficiency and contends that a POSITA would look to Hardjono—arguing that “[i]t would have been obvious to combine Dickinson with Hardjono so that Dickinson’s trust engine returns the assembled data set to the request, as taught by Hardjono.” Pet., 49. More specifically, Petitioner argues that in its proposed combination, “Dickinson’s trust engine assembles the stored segments and returns the reconstructed data ‘[u]pon subsequent receipt of a request for the data’ to the requester [(i.e., Dickinson’s vendor)], as taught by Hardjono.” *Id.*, 26, 45 (“the vendor system 120 ... forwards ... the authentication request to the trust engine” and “transaction engine 205 receives the [vendor request]”).² In other words, in Petitioner’s proposed combination, the vendor sends the trust engine an authentication request, the trust engine reconstructs the enrollment authentication data, and then the trust engine sends the enrollment authentication data to the vendor (i.e., the requester).

89. I note that Petitioner’s argument is premised upon the assertion that “Dickinson’s trust engine already reconstructs the data set upon receiving a retrieval request, and failing to forward that reconstructed data to the requester

² To the extent that Petitioner argues that the Dickinson/Hardjono requester is the transaction engine, that argument also fails for the same reasons explained below.

would leave the workflow incomplete and thereby use trust engine's resources inefficiently." *Id.*, 26. I do not see any explanation from Petitioner or Dr. Zadok of why Dickinson's workflow is "incomplete."

90. Dickinson's workflow is not "incomplete." Dickinson's authentication request from the vendor is only asking the trust engine to authenticate user's identity. Ex. 1003 [Dickinson], 37:24-29 ("authentication is the process of proving that a user is who he says he is. . . . The user must demonstrate to the trust engine 110 that he is who he says he is by either: knowing something that only the user should know (knowledge-based authentication), having something that only the user should have (token-based authentication), or by being something that only the user should be (biometric-based authentication)."). When the authentication engine in Dickinson's trust engine receives the portions of enrollment authentication data and then reconstructs the data set, the authentication engine "compares the enrollment authentication data to the current authentication data provided by the user." *Id.*, 28:11-14.

91. Rather than returning the reconstructed enrollment authentication data as the '194 Patent's claims require, the trust engine only returns the result of the authentication comparison. *Id.*, 28:20-24 ("the authentication engine 215 fills in the authentication request with the result of the comparison of STEP 1045. According to one embodiment of the invention, the authentication request is filled

with a YES/NO or TRUE/FALSE result of the authentication process 1000. In STEP 1055 the filled-in authentication request is returned to the vendor for the vendor to act upon, for example, allowing the user to complete the transaction that initiated the authentication request.”). That “YES/NO” or “TRUE/FALSE” response is all the vendor needs to determine whether the user has been authenticated.

92. In Petitioner’s proposed combination, Dickinson’s “enrollment authentication data”—*e.g.*, username/password or biometric information (*see* Ex. 1003 [Dickinson], 27:34-28:5)—would be sent directly to the vendor. *See* Pet., 26-27, 45 (admitting that its proposed combination has Dickinson’s vendor as the requester sending an authentication request to the trust engine and, relying on Hardjono, the reconstructed authentication data is sent back to the requester). I see no reason why Dickinson’s system would benefit from this modification.

93. The vendor merely needs to confirm the user’s identity in order to allow the user to perform a transaction such as “selecting a purchase option, requesting access to a restricted area or device of the vendor system 120, or the like.” Ex. 1003 [Dickinson], 27:18-19. The vendor does not need any information other than that the user’s current authentication data matches the enrollment authentication data, which is confirmed by the trust engine. *Id.*, 27:15-16 (“the authentication process 1000 includes gathering current authentication data from a

user and comparing that to the enrollment authentication data of the user.”); 28:13-24 (authentication engine “compares the enrollment data to the current authentication data provided by the user” and “fills in the authentication request with the result of the comparison”).

94. Indeed, the vendor never even receives the user’s current authentication data and could not perform the comparison between the current and enrollment authentication data itself. *Id.*, 27:34-28:5 (“the user system 105 gathers the current authentication data, potentially including current biometric information, from the user. The user system 105 . . . transfers that data to the trust engine 110.”). Consequently, the vendor would not have any need for the reconstructed enrollment authentication data.

95. In other words, when the Dickinson’s trust engine returns the “result of [that] comparison” to the vendor, (*id.*, 28:20-24), Dickinson’s workflow is complete because the vendor has received what it requested. There simply is no “incomplete” workflow in Dickinson that would benefit from sending the reconstructed data set.

96. Moreover, in my opinion, there are significant drawbacks to Petitioner’s proposed combination.

97. Dickinson’s authentication process is designed to keep the data set secure by “only” allowing it to be “assembled . . . inside the authentication engine”:

Based on the foregoing, the authentication process 1000 advantageously *keeps sensitive data secure* and produces results configured to maintain the integrity of the sensitive data. For example, *the sensitive data is assembled only inside the authentication engine 215*. For example, the enrollment authentication data is undecipherable until it is assembled in the authentication engine 215 by the data assembling module, and the current authentication data is undecipherable until it is unwrapped by the conventional SSL technology and the private key of the authentication engine 215. Moreover, *the authentication result transmitted to the vendor does not include the sensitive data*, and the user may not even know whether he or she produced valid authentication data.

Id., 28:25-31. Sending the reconstructed enrollment authentication data not only outside of the authentication engine, but outside the trust engine to the vendor, would compromise the data set's security. Indeed, some of the largest data breaches in history have been due to authentication storage being breached. *See, e.g.*, Ex. 2034 [UpGuard] 2 (describing “26 Biggest Data Breaches in US History”); 2 (“A team of Russian hackers targeted Yahoo’s database using backdoors, stolen backups, and access cookies to steal records from all user accounts”); 4-5 (“access to private information was allowed without needing verification or authentication procedures.”); 13 (“the entire Exactis database on a public network that was completely unsecured and accessible to everyone.”).

Petitioner's proposed combination thus would result in the significant drawback of failing to keep sensitive data secure.

98. Without any benefit and only significant drawbacks, Petitioner's proposed combination seems to be based solely upon hindsight in my opinion.

99. Thus, in my opinion, Petitioner fails to demonstrate that a POSITA would be motivated to combine Dickinson and Hardjono as proposed.

100. At this stage of the proceedings, my opinions are preliminary. I may further develop these opinions or offer additional opinions after a decision to institute, should the Board decide to do so.

VIII. CONCLUSION

101. Although my complete opinions are set forth above, for convenience I summarize several points of my opinions in conclusion. For the foregoing reasons, based on my expertise and experience and the record of this case that I have reviewed, it is my opinion that:

- Claims 1-20 are not obvious over Dickinson and Hardjono.

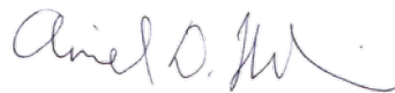
102. I understand that my opinions discussed above support a legal conclusion that claims 1-20 are nonobvious.

In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

I hereby declare that all statements made herein of my own knowledge are true and all statements made herein on information and belief were and are believed by me to be true, and that all statements herein were and are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code and that any such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Respectfully submitted,

Dated: October 17, 2025



Aviel D. Rubin, Ph.D.

EXHIBIT A

Aviel D. Rubin, Ph.D.

Professor Emeritus, Johns Hopkins University
Founder & Managing Partner, Harbor Experts

avirubin@gmail.com

<https://www.linkedin.com/in/avirubin/>



Overview

Avi Rubin is a Computer Scientist with almost a decade of industry experience followed by over 20 years in academia. After receiving his Ph.D. in Computer Science from the University of Michigan in 1994, Dr. Rubin worked as a researcher at Bellcore and then at AT&T Labs. In 2003, he joined the Computer Science faculty at Johns Hopkins University and was promoted to Full Professor with Tenure in 2004. During his over 20 years at Johns Hopkins, Dr. Rubin was Technical Director of the JHU Information Security Institute, along with his regular faculty position. In 2023, he was appointed Computer Science Professor Emeritus at Johns Hopkins. Dr. Rubin is a frequent keynote speaker at industry and academic conferences and delivered widely viewed TED talks in 2011 and 2015. He has testified about information and network security before Congress on multiple occasions and frequently testifies as an expert witness in Federal court. His awards include Fulbright Scholar, Baltimorean of the Year, and the EFF Pioneer Award.

Academic Degrees

- 1994, **Ph.D.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1991, **M.S.E.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1989, **B.S.**, Computer Science (Honors), University of Michigan, Ann Arbor

Academic Appointments

September, 2023 - present

Professor Emeritus, Johns Hopkins University

April, 2004 - August, 2023

Professor (with tenure), Johns Hopkins University

August, 2010 - July, 2011

Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel

January, 2003 - April, 2004

Associate Professor, Johns Hopkins University

January, 2003 - August, 2023

Technical Director, Johns Hopkins University Information Security Institute

2006 - 2010

Director and Principal Investigator (PI), NSF ACCURATE Center

1995 - 1999

Adjunct Professor, New York University

Summer, 1999

Visiting Professor, École Normale Supérieure, Paris, France

1988 - 1993

Teaching Assistant, University of Michigan

Doctoral Committees

Doctoral Thesis Advisor: David Inyangson, JHU

Doctoral Thesis Advisor: Logan Kostick, JHU

Doctoral Thesis Advisor: Atheer Almogbil, JHU (May, 2024)

Doctoral Thesis Advisor: Tushar Jois, JHU (May, 2023)

Doctoral Thesis Advisor: Random Gwinn, JHU (May, 2022)

Doctoral Thesis Advisor: Karl Siil, JHU (May, 2022)

Doctoral Thesis Advisor: James Cervini, JHU (May, 2022)

Doctoral Thesis Advisor: Jeff Chavis, JHU (May, 2021)

Doctoral Thesis Advisor: Gabe Kaptchuk, JHU (May, 2020)

Dissertation Committee: Thomas Tantillo, JHU (September, 2018)

Doctoral Thesis Advisor: Paul Martin, JHU (February, 2016)

Doctoral Thesis Advisor: Michael Rushanan, JHU (May, 2016)

Doctoral Thesis Advisor: Ayo Akinyele, JHU (December, 2013)

Doctoral Thesis Advisor: Matthew Pagano, JHU (August, 2013)

Doctoral Thesis Advisor: Ryan Gardner, JHU (August, 2009)

Doctoral Thesis Advisor: Sam Small, JHU (May, 2009)

Doctoral Thesis Advisor: Sujata Doshi, JHU (May, 2009)

Doctoral Thesis Advisor: Joshua Mason, JHU (June, 2009).

Dissertation Committee: J. Alex Halderman, Princeton University (May, 2009).

Dissertation Committee: Sophie Qiu (May, 2007).

Doctoral Thesis Advisor: Adam Stubblefield (April, 2005).

Dissertation Committee: Kevin FU, MIT (February, 2005).

Dissertation Committee: Robert Fischer, Harvard University (June, 2003).

Dissertation Committee: Marc Waldman, New York University, (April, 2003).

Dissertation Committee: Patrick McDaniel, U. of Michigan (September, 2001).

Doctoral Thesis Advisor: Fabian Monroe, New York University (April, 1999).

Dissertation Committee: Mike Just, Carleton University (November, 1998).

Dissertation Committee: Trent Jaeger, University of Michigan (October, 1996).

Industry Experience

2011 – present

Harbor Experts, Founder & Managing Partner

Harbor Labs, Founder

2005 - 2011

Independent Security Evaluators, Founder & President

1997 - 2002

AT&T Labs -- Research, Secure Systems Research Department

1994 - 1996

Bellcore, Cryptography and Network Security Research Group

Summer, 1990

Great Lakes Software Co., Programmer, Howell, MI

Summer, 1989

IBM, Programmer, Meyers Corners Lab, Poughkeepsie, NY

Books

- Aviel D. Rubin, *Brave New Ballot*, Random House, (September, 2006).
- William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2e)*, Addison Wesley Publishing Company, Inc., (February, 2003).
- **Chapter 4**, *Communications Policy and Information Technology: Promises, Problems, Prospects*, MIT Press, Lorrie Faith Cranor and Shane Mitchell Greenstein, eds., (2002).
- Aviel D. Rubin, *Whitehat Security Arsenal*, Addison Wesley Publishing Company, Inc., (June, 2001).
- **Chapter 8**, Publius and **Chapter 14**, Trust in Distributed Systems, Marc Waldman, Lorrie Faith Cranor, and Aviel D. Rubin, *PeertoPeer*, O'Reilly & Associates, Inc., (February, 2001).
- Aviel D. Rubin, Daniel Geer, Marcus J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, Inc., (June, 1997).
- **Ph.D. dissertation: *Nonmonotonic Cryptographic Protocols***, University of Michigan, Ann Arbor (April, 1994).

Refereed Journal Publications

- David Kotz, Kevin Fu, Carl Gunter, Avi Rubin, *Security for Mobile and Cloud Frontiers in Healthcare*, Communications of the ACM (July, 2015).
- Ayo Akinyele, Christina Garman, Matthew D. Green, Ian Miers, Matthew Pagano, Aviel D. Rubin, Michael Rushanan, *Charm: A Framework for Rapidly Prototyping Cryptosystems*, Journal of Cryptographic Engineering (JCEN), (January, 2013).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *Detecting Code Alteration by Creating a Temporary Memory Bottleneck*, IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, (December, 2009).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin, *Anonymity in Wireless Broadcast Networks*, International Journal of Network Security (IJNS), (January, 2008).
- Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green, *Security Through Legality*, Communications of the ACM (June, 2006).
- Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security*, Electronic Commerce Research Journal, February, 2005.
- David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *Analyzing Internet Voting Security*, Communications of the ACM (October, 2004).

- Simon Byers, Aviel D. Rubin, and David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Transactions on Internet Technology (TOIT), August, 2004.
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)* ACM Transactions on Information and System Security, May, 2004.
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, Communications of the ACM (December, 2002).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *The Architecture of Robust Publishing Systems*, ACM Transactions on Internet Technology (TOIT), (November, 2001).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single-Signon Protocol*, Computer Networks, (July, 2000).
- Christian Gilmore, David P. Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, IEEE Network, (November, 1999).
- Fabian Monrose and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, Future Generation Computer Systems, (March, 2000).
- Michael K. Reiter and Aviel D. Rubin, *Anonymity Loves Company: Anonymous Web Transactions with Crowds*, Communications of the ACM (February, 1999).
- Aviel D. Rubin and Daniel E. Geer, Jr., *Mobile Code Security*, IEEE Internet Computing (November/December, 1998).
- Aviel D. Rubin and Daniel E. Geer, Jr., *A Survey of Web Security*, IEEE Computer, (September, 1998).
- Michael K. Reiter and Aviel D. Rubin, *Crowds: Anonymity for Web Transactions*, ACM Transactions on Information and System Security, (June, 1998).
- Aviel D. Rubin, *An Experience Teaching a Graduate Course in Cryptography*, Cryptologia (April, 1997).
- Aviel D. Rubin, *Extending NCP for public Key Protocols*, Mobile Networks and Applications (ACM/Balzer), 2(3) (April, 1997).
- Aviel D. Rubin, *Independent One-Time Passwords*, USENIX Journal of Computer Systems (February, 1996).
- Aviel D. Rubin, *Secure Distribution of Documents in a Hostile Environment*, Computer Communications (June, 1995).

Refereed Conference Publications

- David Inyangson, Aditya Gaur, Atheer Almogbil, Tushar Jois, Aviel D. Rubin, *SoK: Security in the Inaudible World*, ACM Conference on Security and Privacy in Wireless and Mobile Networks 2025 (WiSec '25), (July, 2025).
- Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, Gabriel Kaptchuk, Aviel D. Rubin, *SocloTy: Practical Cryptography in Smart Home Contexts*, Privacy Enhancing Technologies Symposium 2024 (PETS '24), (July, 2024).
- Atheer Almogbil, Momo Steele, Sofia Belikovetsky, Adil Inam, Olivia Wu, Aviel Rubin, Adam Bates, *Using Behavior Monitoring to Identify Privacy Concerns in Smarthome Environments*, NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec), (February, 2024).

- Samra Kasim, Nawal Valliani, Nelson Ka Ki Wong, Shahin Samadi, Lanier Watkins and Aviel Rubin, *Explainable Autonomic Cybersecurity for Industrial Control Systems*, IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), (March, 2023).
- Valeti Manoj, Shao Wenda, Niu Sihan, Christopher Rouff, Lanier Watkins, Aviel Rubin, *Cybersecurity as a Tic-Tac-Toe Game Using Autonomous Forwards (Attacking) And Backwards (Defending) Penetration Testing in a Cyber Adversarial Artificial Intelligence System*, IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM), (October, 2022).
- James Cervini & Aviel D. Rubin, *Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack*, ICCWS 17th International Conference on Cyber Warfare and Security, (July, 2022).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Make Steganography Great Again — Before It's Too Late*, Real World Crypto 2022, (April, 2022).
- James Cervini, Daniel Muller, Alexander Beall, Joseph Maurio, Aviel Rubin & Lanier Watkins, *A Backfit Approach for Trusted Virtualization-Based Programmable Logic Controller Resilience*, Sixteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, (March, 2022).
- Hedin Beattie, Lanier Watkins, William H. Robinson, Aviel Rubin, Shari Watkins, *Measuring and Mitigating Bias in AI-Chatbots*, 2022 IEEE International Conference on Assured Autonomy (ICAA'22), (March, 2022).
- Random Gwinn, Mark Matties, Aviel D. Rubin, *Wavelet Selection and Employment for Side-Channel Disassembly*, IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), (December, 2021).
- Karl A Siil , Aviel D. Rubin , Matthew C. Elder, Anton T Dahbura, Matthew Green, Lanier Watkins, *Cost-Effective Mission Assurance Engineering Through Simulation*, The 2021 International Conference on Internet of Things and Intelligence Systems (IoTIS'21), (November, 2021).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Meteor: Cryptographically Secure Steganography for Realistic Distributions*, 28th ACM Conference on Computer and Communications Security (CCS '21), (November, 2021).
- James Schaffter, Aviel Rubin and Lanier Watkins, *A Containerization-Based Backfit Approach for Industrial Control System Resiliency*, SafeThings '21 Workshop, (May, 2021).
- Tushar Jois, Claudia Moncaliano, Khir Henderson, Aviel D. Rubin, *WDPKR: Wireless Device Profiling Kit and Reconnaissance*, 2021 Hot Topics in the Science of Security (HotSoS) Symposium (April, 2021).
- Lanier Watkins, ChangHao Cho, John Hurley, Aviel D. Rubin, *Collaborative Global Impact Cloud Computing Risk Assessment Framework*, International IoT, Electronics and Mechatronics Conference (IEMTRONICS '21), (April, 2021).
- Jeffrey S. Chavis, Malcom Doster, Michelle Feng, Syeda Zeeshan, Samantha Fu, Elizabeth Aguirre, Antonio Davila, Kofi Nyarko, Aaron Kunz, Tracy Herriotts, Daniel Syed, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Voice Assistant for IoT Cybersecurity*, Integrated STEM Education Conference (ISEC '21), (March, 2021).
- Lanier Watkins, Danzel Hamilton, Kevin Kornegay, Aviel Rubin, *Triaging Autonomous Drone Faults by Simultaneously Assuring Autonomy and Security in Autonomous*

Drones, 55th Annual Conference on Information Sciences and Systems (CISS '21), (March, 2021).

- Lanier Watkins, James Ballard, Kevin Hamilton, William H. Robinson, Aviel Rubin, Cleon Davis, *Bio-Inspired, Host-based Firewall* (Refereed WIP paper), 23rd IEEE International Conference on Computational Science and Engineering (CSE), (December, 2020).
- Lanier Watkins, Yue Yu, Sifan Li, William H. Robinson, Aviel D. Rubin, *Using Deep Learning to Identify Security Risks of Personal Mobile Devices in Enterprise Networks*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).
- Lanier Watkins, Kevin D. Fairbanks, Chengyu Li, Mengdi Yang, William H. Robinson, Aviel D. Rubin, *A Black Box Approach to Inferring Characterizing, and Breaking Native Device Tracking Autonomy*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).
- Karl Siil, Aviel Rubin, Matthew Elder, Anton Dahbura, Matthew Green, Lanier Watkins, *Mission Assurance for Autonomous Undersea Vehicles*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Jeffrey Chavis, Aaron Kunz, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Capability for Autonomous IoT System Security: Pushing IoT Assurance to the Edge*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Lanier Watkins, Shane Sartalamacchia, Richard Bradt, Karan Dhareshwar, Harsimar Bagga, William H. Robinson, Aviel Rubin, *Defending Against Consumer Drone Privacy Attacks: A Blueprint For A Counter Autonomous Drone Tool*, ISOC Workshop on Decentralized IoT Systems and Security (DISS 2020), (February, 2020).
- Adrian Cartagena, Gerald Rimmer, Thomas Van Dalsen, Lanier Watkins, William H. Robinson, Aviel D. Rubin, *Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Jeffrey Chavis, Lanier Watkins, Anna Buczak, Aviel D. Rubin, *Connected Home Automated Security Monitor (CHASM): Protecting IoT Through Application of Machine Learning*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Lanier Watkins, Shreya Aggarwal, Omotola Akeredolu, William H. Robinson and Aviel D. Rubin, *Tattle Tail Security: An Intrusion Detection System for Medical Body Area Networks*, Workshop on Decentralized IoT Systems and Security (DISS '19), (February, 2019).
- Lanier Watkins, Juan Ramon, Gaetano Snow, Jessica Vallejo, William H. Robinson, Aviel D. Rubin, Joshua Ciocco, Felix Jedrzejewski, Jinglun Liu, Chengyu Li, *Exploiting Multi-Vendor Vulnerabilities as BackDoors to Counter the Threat of Rogue Small Unmanned Aerial Systems*, ACM Workshop on Mobile IoT Sensing, Security, and Privacy (Mobile IoT SSP '18), (June, 2018).
- Paul D. Martin, David Russel, Malek Ben Salem, Stephen Checkoway, Aviel D. Rubin, *Sentinel: Secure Mode Profiling and Enforcement for Embedded Systems*, Proc. ACM/IEEE International Conference on Internet-of-Things Design and Implementation, (April, 2018).

- Gabriel Kaptchuk, Matthew D. Green and Aviel D. Rubin, *Outsourcing Medical Dataset Analysis: A Possible Solution*, Financial Cryptography Conference, (April, 2017).
- Michael Rushanan, David Russell and Aviel D. Rubin, *Mallory-Worker: Stealthy Computation and Covert Channels using Web Workers*, Proceedings of the 12th International Workshop on Security and Trust Management, (September, 2016).
- Paul Martin, Michael Rushanan, Thomas Tantillo, Christoph Lehmann and Aviel Rubin, *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics, (October, 2016).
- Gabriel Kaptchuk and Aviel D. Rubin, *A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker*, Proceedings of the 15th Annual Security Conference, (March, 2016).
- Aviel D. Rubin, *Taking Two-Factor to the Next Level: Protecting Online Poker, Banking, Healthcare and Other Applications*, Proceedings of the 2014 Annual Computer Security Applications Conference, Invited Keynote Essay, (December, 2014).
- Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy-SoK Track (May, 2014).
- Christina Garman, Matthew Green, Ian Miers, Aviel D. Rubin, *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity*, 1st Workshop on Bitcoin Research (March, 2014).
- Paul Martin, Aviel Rubin and Rafae Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control*, Health Informatics Symposium at the ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics, (September, 2013).
- Ian M. Miers, Christina Garman, Matthew D. Green, Aviel D. Rubin, *Zerocoin: Anonymous Distributed e-Cash from Bitcoin*, Proc. IEEE Symposium on Security and Privacy (May, 2013).
- Ian M. Miers, Matthew D. Green, Christoph U. Lehmann, Aviel D. Rubin, *Vis-à-Vis Cryptography: Private and Trustworthy In-Person Certifications*, In Proceedings of the 3rd USENIX/HealthSec Workshop, (August, 2012).
- Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N. J. Peterson and Aviel D. Rubin, *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, (October, 2011).
- Matthew D. Green, Aviel D. Rubin, *A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report 4-page Extended Abstract*, In Proceedings of the 2nd USENIX/HealthSec Workshop, (August, 2011).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Designing for Audit: A Voting Machine with a Tiny TCB*, Financial Cryptography Conference, (January, 2010).
- Ryan Gardner, Sujata Garera, Matthew W. Pagano, Matthew D. Green, Aviel D. Rubin, *Securing Medical Records on Smart Phones*, Workshop on Security and Privacy in Medical and Home-Care Systems, (November, 2009).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Coercion Resistant End-to-end Voting*, Financial Cryptography Conference, (February, 2009).

- Ryan Gardner, Sujata Garera, Anand Rajan, Carols Rozas, Aviel D. Rubin, Manoj Sastry, *Protecting Patient Records from Unwarranted Access*, Future of Trust in Computing, (July, 2008).
- Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, 5th ACM Workshop on Recurring Malcode (WORM '07), (November, 2007).
- Sujata Garera and Aviel D. Rubin, *An Independent Audit Framework for Software Dependent Voting Systems*, 14th ACM Conference on Computer and Communications Security, (November, 2007).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *On the Difficulty of Validating Voting Machine Software with Software*, In Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), (August, 2007).
- Sujata Doshi, Fabian Monrose, and Aviel D. Rubin, *Efficient Memory Bound Puzzles using Pattern Databases*, 4th International Conference on Applied Cryptography and Network Security (ACNS'06), (June, 2006).
- Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Aviel Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, (June 2006).
- Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Aviel D. Rubin, *Secure Deletion for a Versioning Filesystem*, Proc. USENIX Conference on File and Storage Technologies (FAST '05), (December, 2005).
- Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, *Security Analysis of a Cryptographically-Enabled RFID Device*, 14th USENIX Security Symposium, (August, 2005).
- Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004).
- Nathanael Paul, David Evans, Aviel D. Rubin and Dan Wallach, *Authentication for Remote Voting*, ACM Workshop on Human-Computer Interaction and Security Systems (April, 2003).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Aviel Rubin, *Protocols for Anonymity in Wireless Networks*, Proc. 11th International Workshop on Security Protocols (April, 2003).
- Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2003).
- Simon Byers, Aviel D. Rubin, David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Workshop on Privacy in the Electronic Society (November, 2002).
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2002).
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), (October, 2001).

- Aviel D. Rubin and Rebecca N. Wright, *Offline generation of limited-use credit card numbers*, Financial Cryptography Conference, (February, 2001).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *Publius, A robust, tamper-evident and censorship-resistant web publishing system*, 9th USENIX Security Symposium, (August, 2000).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Sign-on Protocol*, 9th International World Wide Web Conference, (May, 2000).
- Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, Financial Cryptography Conference, (February, 2000).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device*, 6th ACM Conference on Computer and Communications Security, (November, 1999).
- Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords*, 8th USENIX Security Symposium, (August, 1999).
- Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Fabian Monrose, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground*, Proc. IEEE Symposium on Security and Privacy (May, 1998).
- Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread Email in an Untrusted Network*, Second Australasian Conference on Information Security and Privacy (July, 1997).
- Fabian Monrose and Aviel D. Rubin, *Authentication via Keystroke Dynamics*, 4th ACM Conference on Computer and Communications Security (April, 1997).
- David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1997).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content*, Proc. 6th USENIX Security Symposium (July, 1996).
- Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, Proc. of Eurocrypt '96 (May, 1996).
- Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
- Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
- Aviel D. Rubin, *PseudoRandom Functions for OneTime Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
- Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).

- Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
- Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

- Aviel D. Rubin, "Broadband Certified Mail", **US Patent Numbers 6,990,581**, (January 24, 2006) and 9,876,769, (January 23, 2018).
- Aviel D. Rubin, Utilization of multiple devices to secure online transactions, **US Patent Number 9,064,376**, (June 23, 2015).
- Steven M. Bellovin, Thomas J. Killian, Bruce LaRose, Aviel D. Rubin, Norman L. Schryer, Method and apparatus for connection to virtual private networks for secure transactions, **US Patent Numbers 8,239,531**, (August 7, 2012) and **8,676,916** (March 18, 2014).
- Christian A. Gilmore, David P. Kormann, and Aviel D. Rubin, Method and apparatus for secure remote access to an internal web server, **US Patent Number 7,334,126**, (February 19, 2008).
- Aviel D. Rubin, "Method for secure remote backup", **US Patent Number 7,222,233**, (May 22, 2007).
- Frederick Douglass, Michael Rabinovich, Aviel D. Rubin, and Oliver Spatscheck, "Method for content distribution in a network supporting a security protocol", **US Patent Number 7,149,803**, (December 12, 2006).
- William A. Aiello, Steven M. Bellovin, Charles Robert Kalmanek, Jr., William T Marshal, and Aviel D. Rubin, "Method and apparatus for enhanced security in a broadband telephony network", **US Patent Number 7,035,410**, (April 25, 2006).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, "Using smartcards to enable probabilistic transaction on an untrusted device", **US Patent Number 6,496,808**, (December 17, 2002).
- Aviel D. Rubin and Victor J. Shoup, "Session Key Distribution Using Smart Cards", **US Patent Number 5,809,140**, (September 15, 1998).
- Aviel D. Rubin, "Method for the Secure Distribution of Electronic Files in a Distributed Environment", **US Patent Number 5,638,446**, (June 10, 1997).

Professional Activities

Board of Directors

- Director**, Iron Circle (provide Online Cybersecurity Education), (2025 – present).
- Director**, Maryland Israel Development Center (MIDC), (2013-2018).
- Director**, USENIX Organization, elected by popular vote (2000-2004).

Editorial and Committees

- Chair**: IEEE Security & Privacy Symposium Test of Time Awards Committee for 2008-2010 Conferences, May, 2020.
- Associate Editor**: IEEE Transactions on Information Forensics and Security (2009 - 2011).
- Associate Editor**: Communications of the ACM (CACM), 2009 - 2017.
- Guest Co-Editor**: IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, December 1, 2009.
- Guest Co-Editor**: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting, October/November, 2007.

Associate Editor: IEEE Transactions on Software Engineering (2005-2006). Editorial and **Advisory Board:** International Journal of Information and Computer Security (IJICS) (2004 - 2006).

Guest Co-Editor: IEEE Computer Networks, Special Issue on Web Security, January, 2005. **Editorial Board:** Journal of Privacy Technology (2004-2006).

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting Security, January/February, 2004.

Member: Security Peer Review Group (SPRG) of the Federal Voting Assistance Program's (FVAP) Secure Electronic Registration and Voting Experiment (SERVE) Project, 2003 - 2004.

Member: DARPA Information Science And Technology Study Group (2003 - 2006). **Associate Editor:** IEEE Security & Privacy Magazine (2003 - 2011).

Guest Editor: Communications of the ACM, Special Issue on Wireless Networking Security, May, 2003.

Associate Editor: ACM Transactions on Internet Technology (2002-2005).

Executive Committee Member: DIMACS Workshop Series with Special Focus on Network Security (2002 - 2004).

Advisory Board Member: Information Security and Cryptography Book Series, Springer, 2001- 2006.

Member: Steering Group, ISOC Symposium on Network and Distributed System Security, 2001 - 2004.

Member: Government Infosec Science and Technology Study Group on malicious code, 1999 - 2000.

Member: AT&T Internet Intellectual Property Review Team, 1999 - 2001. **Associate Editor:** Electronic Commerce Research Journal, Baltzer Science Publishers, 1999 - 2002.

CoEditor: Electronic Newsletter of the IEEE Technical Committee on Security & Privacy, with Paul Syverson, 1998.

Editorial Board: Bellcore Security Update Newsletter, 1995 - 1996.

Conference Committees

- **Program committee member:** ACM Workshop on CyberSecurity in Healthcare (HealthSec '25), Honolulu, HI, December 9, 2025.
- **Program committee member:** ACM Workshop on CyberSecurity in Healthcare (HealthSec '24), Salt Lake City, UT, October 14, 2024.
- **Program Committee member:** NDSS Workshop: Innovative Secure IT Technologies Against COVID19, San Diego, CA, February, 2020.
- **Program Committee member:** Financial Cryptography '15 Barbados, February, 2015.
- **Program Committee member:** USENIX HealthTech Workshop on Health Information Technologies (HealthTech '15), August 11, 2015.
- **Program Co-chair:** (w/Eugene Vasserman) USENIX HealthTech Workshop on Health Information Technologies (HealthTech '14), August 19, 2014.
- **Program committee member:** 2nd USENIX Workshop on Health Security & Privacy (HealthSec '11), August 9, 2011.
- **Program Co-chair:** (w/Kevin Fu & Yoshi Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
- **Program Committee member:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.

- **Invited Talks Co-Coordinator:** 17th USENIX Security Symposium, San Jose, CA, July 28 August 1, 2008.
- **Program Co-chair:** (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 1822, 2008.
- **Program Co-chair:** (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.
- **Program Committee member:** Financial Cryptography '04 Key West, Florida, February 9-12, 2004.
- **Program Committee member:** 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
- **Program Committee member:** 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
- **Program Committee member:** 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
- **Program Vice Chair:** Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 2024, 2003.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 1114, 2003.
- **Program Committee member:** Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
- **Program Committee member:** 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRDL), Singapore December 912, 2002.
- **Program Committee member:** ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
- **Program Committee member:** 9th ACM Conference on Computer and Communications Security, Washington D.C., November 1721, 2002.
- **Program Committee member:** 5th International Conference on Electronic Commerce Research (ICECR5), Montreal, Canada, October 2327, 2002.
- **Program Committee member:** 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 1415, 2002.
- **Program Committee member:** 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 1416, 2002.
- **Program Committee member:** 11th USENIX Security Symposium, San Francisco, Ca, August 59, 2002.
- **Program Committee member:** International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 2124, 2002.
- **Program Committee member:** 11th International World Wide Web Conference Honolulu, Hawaii, May 711, 2002.
- **Program Committee member:** 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 1415, 2002.
- **Program Committee member:** The 1st International Workshop on PeertoPeer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 78, 2002.

- **Program Committee member:** The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001. Program Committee member: 10th USENIX Security Symposium, Washington D.C., August 1317, 2001.
- **Program Committee member:** Financial Cryptography '01 Grand Cayman, Cayman Islands, BWI, February, 2001.
- **Program Co-chair:** (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 79, 2001.
- **Program Committee member:** The 3rd International Conference on Telecommunications and Electronic Commerce Dallas, TX, November 1619, 2000. Program Committee member: 9th USENIX Security Symposium, Denver, Colorado, August 1417, 2000.
- **Program Committee member:** Workshop on Design Issues in Anonymity and Unobservability Berkeley, California, July 2526, 2000.
- **Program Committee member:** Performance and Architecture of Web Servers (PAWS), Santa Clara, CA, June 18, 2000.
- **Program Co-chair:** (w/Gene Tsudik): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 24, 2000.
- **Program Committee member:** 1999 International Information Security Workshop (ISW'99), Kuala Lumpur, Malaysia, November 67, 1999.
- **Program Committee member:** 2nd Int'l. Conference on Telecommunications and Electronic Commerce, Nashville, TN, October 68, 1999.
- **Invited Talks coordinator:** 8th USENIX Security Symposium, Washington D.C., August, 1999.
- **Program Chair:** 24th USENIX Annual Technical Conference, Monterey, CA, June 711, 1999.
- **Program Committee member:** 8th International World Wide Web Conference , Toronto, Canada, May 1114, 1999.
- **Program Committee member:** 3rd USENIX workshop on Electronic Commerce , Boston, MA, August 31 September 3, 1998.
- **Program Committee member:** 5th ACM Conference on Computer and Communications Security, San Francisco, CA, November 35, 1998.
- **Program Chair:** 7th USENIX Security Symposium, San Antonio, TX, Jan. 2629, 1998.
- **Program Committee member:** 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 24, 1997.
- **Program Committee member:** 6th USENIX Security Symposium, San Jose, CA, July 2225, 1996.
- **Program Committee member:** ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 2223, 1996.

Panels

- **Panelist:** TLTF Conference: Shielding Your Business: Cybersecurity & Vendor Risk Management, Miami, Florida (December 4, 2024).
- **Panelist:** CyberTech Global Conference: The Post-COVID Cyber Challenges in the Health Sector, UAE-Dubai (April 6, 2021).
- **Panel Organizer and Moderator:** USENIX Security Conference: The 2020 Election: Remote Voting, Disinformation, and Audit (August 12, 2020).
- **Panelist:** Cardozo Society Associated panel: Cybersecurity and Privacy Law in the Digital Era, Baltimore, MD (February 19, 2020).

- **Panelist:** Washington Post panel: Hacking Health, Washington DC (June 14, 2016).
- **Panelist:** Financial Cryptography Conference, Security & Privacy, Barbados (February 24, 2016).
- **Panelist:** RSA Conference, Social Networks Security Panel, San Francisco, CA (April 21, 2015).
- **Panelist:** Expert Witness in Mock Trial: FTC Data Security, 63rd American Bar Association Section of Antitrust Law Spring Meeting Washington DC, (April 15, 2015).
- **Panelist:** Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
- **Panelist:** Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).
- **Panelist:** Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
- **Panelist:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
- **Panelist:** Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
- **Panelist:** Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel (May 18, 2009).
- **Panelist:** RSA Conference, Exploiting Online Games, San Francisco, CA (April 23, 2009).
- **Panelist:** American Association for the Advancement of Science, Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel, Washington DC, (November 27, 2006).
- **Panelist:** California Secretary of State's Voting System Testing Summit, Security Panel, Sacramento, CA, (November 28, 2005).
- **Panelist:** NIST Symposium on Voting System Threats, Configuration and Usability Threats, Gaithersburg, MD, (October 7, 2005).
- **Panelist:** Conference of State Supreme Court Chief Justices, Voting Technologies, Charleston, SC (August 1, 2005).
- **Panelist:** Workshop on observation of automated elections, The Carter Center, Atlanta, GA (March 18, 2005).
- **Panelist:** The Carter Center Venezuela Virtual Panel, (November, 2004).
- **Panelist:** Workshop on Voting, Vote Capture and Vote Counting, Harvard Kennedy School of Government, The Technologies of Voting, Cambridge, MA (June 1, 2004).
- **Panelist:** Computer Science and Telecommunications Board of The National Academy of Science Workshop on Dependable Software Systems, Case Study: Electronic Voting Washington D.C. (April 20, 2004).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** Democracy Now, 2003, Voter-Verifiable Elections: How Do We Get There?, Washington D.C. (November 23, 2003).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** IEEE Infocom 2002, Securing Wireless and Mobile Networks, Is It Possible?, New York City (June 25, 2002).
- **Participant:** 2002 Security Visionary Roundtable: A Roadmap for a Safer Wireless World, Washington D.C., (May 5-7, 2002).

- **Panelist:** Computers Freedom and Privacy 2002, Who Goes There? Privacy in Identity and Location Services, San Francisco (April 18, 2002).
- **Panel moderator:** Conference on Democracy and the Internet in an Enlarging Europe Overview of On-Line Voting: Systems and Issues, New York, NY (March, 2001).
- **Panelist:** Financial Cryptography 2001, The Business of Electronic Voting, Grand Cayman (February, 2001).
- **Panelist:** National Science Foundation E-voting workshop, Washington, D.C., (October, 2000).
- **Panelist:** 5th ACM Conference on Computer and Communications Security, Anonymity on the Internet, San Francisco, CA, (November, 1998).
- **Panelist:** Open Systems Security and ISSA Annual Conference, Securing the Web, Orlando, FL (March, 1998).
- **Panel organizer and moderator:** Implementation Issues for Electronic Commerce: What Every Developer Should Know. ISOC Symposium on Network and Distributed System Security, (March, 1998).
- **Panel organizer and moderator:** Downloadable Executable Content Past, Present and Future. ISOC Symposium on Network and Distributed System Security (February, 1997).
- **Panelist:** DIMACS Workshop on Network Threats, Web/Java Security Issues, New Brunswick, NJ (December 5, 1996).

Testimony

Before Government Bodies

- United States House Committee on Administration, Full Committee Hearing, Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House, Live via WebEx, (July 17, 2020).
- Maryland House, Expert Testimony, Hearing on HB 888, Consumer Protection, Security Features for Connected Devices, Economic Matters Committee, Annapolis, MD, (February 26, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 443 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 19, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 553/HB 1276 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 26, 2019). United States Pentagon, High Level Security Briefing on the Security of Embedded Devices (January 15, 2014).
- United States House Committee on Science, Space, and Technology, Full Committee Hearing Is My Data on Healthcare.gov Secure?, Washington, D.C., (November 19, 2013).
- United States House Committee on Oversight and Government Reform, hearing on electronic voting, Washington, D.C., (April 18, 2007).
- United States House Committee on Appropriations, hearing on ensuring the integrity of elections, Washington, D.C., (March 7, 2007).
- Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, Hearing on Senate Bill 392 for VoterVerified Records in Voting Systems, Annapolis, MD, (February 22, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 18 for improving voting systems in Maryland, Annapolis, MD, (February 1, 2007).

- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland, Annapolis, MD, (February 1, 2006).
- United States Election Assistance Commission, Hearing on Voluntary Voting Systems Guidelines, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).
- Senate hearing: Voting in 2004: A Report to the Nation on America's Election Process, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
- United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, Public Hearings on Computer Security and Transparency, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).
- United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, Hearing on Electronic Voting, Washington, D.C. (July 20, 2004).
- United States House Committee on House Administration, Expert Testimony, Hearing on Security of Electronic Voting, Washington, D.C. (July 7, 2004).
- United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
- United States Election Assistance Commission, Expert Testimony, Hearing on Electronic Voting Security, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

- **Genius Sports Ltd.** vs. SportsCastr Inc., IPR2024-01311, Cahill Gordon & Reindel, US Patent Trial and Appeal Board. (Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (August 14, 2025).
- **Proxense, LLC**, vs. Microsoft Corporation, Case # 6:23-cv-00319-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (May 13, 2025).
- **US Dominion, Inc.** vs. Sidney Powell P.C., Case # 1:21-cv-00040-CJN-MAU, Susman Godfrey, United States District Court, District of Columbia. (Defamation)
 - Expert Testimony at deposition, Annapolis, MD (April 11, 2025).
- **US Dominion, Inc.** vs. Herring Networks, Inc, Case # 1:21-cv-02130-CJN-MAU, Susman Godfrey, United States District Court, District of Columbia. (Defamation)
 - Expert Testimony at deposition, Annapolis, MD (April 10, 2025).
- Zoll Data Systems, Inc. vs. **Wave/Experian**, Case # 24-cv-00584-DDD-KAS, Jones Day, United States District Court, Central District of Colorado (Trade Secret)
 - Expert Testimony at Preliminary Injunction hearing, Denver, CO (February 27, 2025).
- Datavant, Inc. vs. **Vigilytics LLC**, IPR2024-00381, Fish & Richardson, US Patent Trial and Appeal Board. (Patent Validity)
 - Expert Testimony at deposition, Stuart, FL (February 17, 2025).
- **WSOU Investments, LLC**, vs. Cisco Systems Inc., Case # 6:21-cv-00128-ADA; Susman Godfrey/Folio Law Group, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)

- Expert Testimony at Trial, Waco, Texas (February 10 & 11, 2025).
- Expert Testimony at deposition, Annapolis, MD (March 30, 2023).
- Expert Testimony at deposition, Annapolis, MD (January 18 & 19, 2023).
- Meta Platforms, Inc. vs. **Sitnet LLC**, IPR2024-00529, IPR2024-00530, IPR2024-00528, IPR2024-00612, Hecht Partners, US Patent Trial and Appeal Board. (Patent Validity)
 - Expert Testimony at deposition, Austin, TX (February 7, 2025).
- **US Dominion, Inc.** vs. Newsmax Media Inc, Case # N21C-08-063 EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
 - Expert Testimony at deposition, West Palm Beach, FL (February 4, 2025).
- Dr. Rachel Kent, Class Representative vs. **Apple Inc, Apple Distribution International Limited**, Case # 1403/7/7/21, Gibson Dunn, Competition Appeal Tribunal, London, England. (App Store Security & Privacy)
 - Expert Testimony at Trial, London, England (January 27-28, 2025).
- **Virtru Corporation** vs Microsoft Corporation, Case #1:22-cv-01309-DAE; Morrison & Foerster, United States District Court, Western District of Washington.
 - Expert Testimony at deposition, Stuart, FL (December 20, 2024). (Patent Secondary Consideration and Non-infringing alternatives)
 - Expert Testimony at deposition, Stuart, FL (December 19, 2024). (Patent infringement)
- Google LLC vs. **Security First Innovations**, IPR 2024-00212, IPR 2024-00214, IPR 2024-00215, Sullivan & Cromwell, US Patent Trial and Appeal Board. (Patent Validity)
 - Expert Testimony at deposition, Stuart, FL (December 12, 2024).
- Datavant, Inc vs. **Vigilitics, LLC**, IPR 2024-00226, Fish & Richardson, US Patent Trial and Appeal Board. (Patent Validity)
 - Expert Testimony at deposition, Stuart, FL (November 22, 2024).
- **Proxense, LLC**, vs. Google., Case # 6:23-cv-00320-ADA; Susman Godfrey, United States District Court, Western District of Texas.
 - Expert Testimony at deposition, Annapolis, MD (October 23, 2024), (Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (October 22, 2024), (Patent infringement)
 - Expert Testimony at deposition, Key West, FL (December 18, 2023), (Patent claim construction)
- Robocast vs. **Netflix Inc**, Case # 1:22-cv-00305-JLH-CJB, Latham & Watkins, United States District Court, District of Delaware. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Washington DC, (August 28, 2024).
- Epic Games, Inc & Anor vs. **Apple Inc & Anor.**, Case # NSD 1236 of 2020, Gibson Dunn, Federal Court of Australia, District of New South Wales. (App Store Security & Privacy)
 - Expert Testimony at Trial, Melbourne, Australia (May 29, 2024).
- **Softex LLC** vs Absolute Software Corporation, Dell Technologies Inc, and HP Inc, Case # 1:22-cv-01309-DAE; McKool Smith, United States District Court, Western District of Texas. (Patent Claim Construction)
 - Expert Testimony at deposition, Key West, FL (November 27, 2023).

- **Milliman, Inc** and Vigilytics LLC, vs. Gradient A.I. Corp., Case # 1:21-cv-10865-NMG; K&L Gates, United States District Court, District of Massachusetts. (Patent Claim Construction, Patent Infringement, Patent Validity, Trade Secret)
 - Expert Testimony at deposition, Annapolis, MD (November 27, 2023).
 - Expert Testimony at deposition, Annapolis, MD (November 17, 2022).
- Microsoft Corporation vs. **Mediapointe, Inc**, Case # 2:22-cv-01009-MCS-MRW; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2023).
- Akamai Technologies, Inc vs. **Mediapointe, Inc**, Case # 2:22-cv-06233-MCS-AFM; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 22, 2023).
- Lauri Valjakka vs. **Netflix Inc**, Case # 4:22-cv-01490-JST, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Annapolis, MD (September 8, 2023).
- **TecSec Inc** vs. Oracle, Case # 1:10CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (June 13, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 11, 2020).
- Global Eticket Exchange Ltd. vs. **TicketMaster LLC**, Case # 6:21-cv-00399-ADA, Fish & Richardson, United States District Court, Western District of Texas. (Patent Non-infringement and validity)
 - Expert Testimony at Trial, Waco, TX (May 3, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 31, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 16, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01306, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 20, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01307, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 19, 2023).
- **TecSec Inc** vs. Cisco, Case # 1:10-CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Washington DC (April 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 14, 2020).
- Finjan vs. **Palo Alto Networks**, Case # 4:14-CV-04908-PJH, Morrison and Foerster, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Annapolis, MD (March 17, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Annapolis, MD (March 15, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Pikesville, MD (August 16, 2021). (*Claim Construction*)

- Centripetal Networks, Inc. vs. **Keysight Technologies, Inc.**, Investigation No. 337-TA-1314-MJM, Reed Smith LLP, United States International Trade Commission (ITC). (Patent Non-infringement & Domestic Industry Technical Prong)
 - Expert Testimony at Trial, Washington DC (March 6, 2023).
 - Expert Testimony at Deposition, Las Vegas, NV (December 2, 2022).
- **Proxense, LLC**, vs. Samsung Electronics Co., Case # 6:21-cv-00210ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (January 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 30, 2022).
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2022).
- **US Dominion, Inc.** vs. Fox News Network, Case # N21C-03-257-EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
 - Expert Testimony at deposition, Annapolis, MD (January 10, 2022).
- **Rimini Street, Inc.** vs. Oracle International Corporation, et. al., Case # 2:14-CV-01699 LRHCWH, Gibson Dunn, United States District Court, District of Nevada. (Software security)
 - Expert Testimony at trial, Las Vegas, NV (December 9, 2022).
 - Expert Testimony at deposition, Baltimore, MD (August 30, 2018).
- **IOEngine, LLC**, vs. Ingenico Inc., Case # 1:18-cv-826 WCB; Dechert LLP, United States District Court, District of Delaware. (Patent Infringement & Patent Validity)
 - Expert Testimony at trial, Wilmington, DE (July 12 & 14, 2022).
 - Expert Testimony at deposition, Annapolis, MD (January 28, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 19, 2022).
- **WSOU Investments, LLC**, vs. Microsoft Corporation, Case # 6:20-cv-00464-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (May 15 & 16, 2022).
- **10Tales Inc.** vs. TikTok PTE. LTD., Case # 4:21-cv-3868-YGR; Cozen O'Connor, United States District Court, Northern District of California. (Patent Claim Construction)
 - Expert Testimony at deposition, Annapolis, MD (May 11, 2022).
- **IOEngine, LLC**, vs. PayPal Holdings, Inc., Case # 1:18-cv-452-WCB; Dechert LLP, United States District Court, District of Delaware. (Patent infringement)
 - Expert Testimony at deposition, Bonita Springs, FL (January 18, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 26, 2022).
- AGIS Software Development LLC vs. **Uber Technologies Inc.**, Case # 2:21-cv-00026-JRG-RSP, Gibson Dunn, United States District Court, Eastern District of Texas. (Non-infringement)
 - Expert Testimony at Deposition, Annapolis, MD (December 22, 2021).
- Sable Networks vs. **Splunk Inc.**, Case # 5:21-CV-00040-RWS, Morrison and Foerster, United States District Court, Eastern District of Texas. (Claim Construction)
 - Expert Testimony at Deposition, Annapolis, MD (December 13, 2021).
- Huawei Technologies Co. vs. **Verizon Communications Inc.**, Case # 6:20-CV-00090, Quinn Emanuel, United States District Court, Western District of Texas. (Patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Pikesville, MD (July 1, 2021).

- Epic Games, Inc. vs. **Apple Inc.**, Case # 4:20-cv-05640-YGR-TSH, Gibson Dunn, United States District Court, Northern District of California. (Sherman Act)
 - Expert Testimony at Trial, Oakland, CA (May 20-21, 2021).
 - Expert Testimony at Deposition, Pikesville, MD (March 26, 2021).
- Philips North America LLC ; Koninklijke Philips N.V. vs. **Summit Imaging Inc.**, Case # 2:19cv01745JLR, Seed IP, United States District Court, Western District of Washington at Seattle. (DMCA and Copyright)
 - Expert Testimony at deposition, Pikesville, MD (March 16, 2021).
- **California Physicians Service, Inc D/B/A Blue Shield of California** vs. Healthplan Services Inc, Case # 3:18-cv-3730 Latham & Watkins, United States District Court, Northern District of California. (Contract Dispute: Software Quality and Security)
 - Expert Testimony at Deposition, Pikesville, MD (March 9, 2021).
- Finjan vs. **Qualys Inc.**, Case # 4:18-cv-07229-YGR, Wilson Sonsini, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at Deposition, Pikesville, MD (March 4, 2021).
- Finjan vs. **Sonicwall Inc.**, Case # 5:17-cv-04467-BLF-HRL, Duane Morris, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Pikesville, MD (October 30, 2020).
 - Expert Testimony at deposition, Pikesville, MD (October 29, 2020).
- **Blackberry Limited** vs. Facebook, Inc, Case #2:18-cv-01844 (KSx), Quinn Emanuel Urquhart & Sullivan, LLP, United States District Court, Central District of California. Expert Testimony at Deposition, Baltimore, MD (December 20, 2019). (patent infringement & patent validity)
- **Netfuel, Inc.** vs. Cisco Systems, Inc, Case # 5:18-cv-2352-EJD, Susman Godfrey, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 16 & 17, 2019). (patent infringement & patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (June 11, 2019). (patent infringement)
 - Expert Testimony at Markman Hearing, San Jose, CA (February 28, 2019). (courtroom tutorial)
 - Expert Testimony at deposition, Baltimore, MD (December 20, 2018). (claim construction)
- **Symantec Corporation** vs. Zscaler, Inc., Case # 3:17-CV-04414-JST, Baker Botts, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 6, 2019). (patent infringement)
 - Expert Testimony at Deposition, Baltimore, MD (August 2, 2019). (Assignor Estoppel)
- Koninklijke Philips vs. **Microsoft Inc**, Case # 4:18-cv-01885-HSG, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Baltimore, MD (July 17, 2019).

- **Cypress Lake Software, Inc. vs. Samsung Electronics & Dell Inc**, Case # 6:18-cv-030-JKD and 6:18cv0138JDK, Garteiser Honea, United States District Court, Eastern District of Texas. (patent infringement and patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (July 1011, 2019).
- **Finjan vs. Juniper Networks**, Case # 3:17-cv-05659-WHA , Irell and Manella, United States District Court, Northern District of California.
 - Expert Testimony at deposition, Baltimore, MD (April 2, 2019). (patent Non-infringement)
 - Expert Testimony at deposition, San Francisco, CA (March 9, 2019). (patent Non-infringement)
 - Expert Testimony at trial, San Francisco, CA (December 13, 2018). (patent Non-infringement and invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 9, 2018). (patent Non-infringement and invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 6, 2018). (patent Non-infringement)
 - Expert Testimony at deposition, Baltimore, MD (June 12, 2018). (patent Non-infringement)
- **Grace et. al. vs. Apple Inc.**, Case # 5:17-CV-00551LHK (NC), Durie Tangri, United States District Court, Northern District of California. (class action)
 - Expert Testimony at deposition, Towson, MD (September 26, 2018).
- **Grace et. al. vs. Apple Inc.**, Case # 5:17-CV-00551-LHK (NC), Kirkland & Ellis, United States District Court, Northern District of California. (class certification)
 - Expert Testimony at deposition, Pikesville, MD (July 3, 2018).
- **F5 Networks, Inc. vs. Radware, LTD.**, IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (January 24, 2018).
- **Amazon.com Inc., Hulu, LLC, and Netflix, Inc. vs. Uniloc Luxembourg S.A.**, IPR 201700948, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (October 9, 2017).
- **Phishme, Inc. vs. Wombat Technologies, Inc.**, Case # 16403-LPS-CJB, K&L Gates, United States District Court, Delaware. (patent claim construction)
 - Expert Testimony at deposition, Washington DC, (October 5, 2017).
- **Finjan vs. Symantec Corporation.**, Case # 14-cv-02998-HSG, Quinn Emanuel, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Baltimore, MD (September 14-15, 2017).
- **Kudelski SA, Nagra USA, Inc., NagraVision SA, and OpenTV, Inc. vs. Comcast Corporation**, Case # 2:16-cv-1362-JRG, Covington, United States District Court, Eastern District of Texas. (patent claim construction).
 - Expert Testimony at deposition, Baltimore, MD (September 1, 2017).
- **F5 Networks, Inc. vs. Radware, LTD.**, IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 10, 2017).

- Intellectual Ventures vs. **JP Morgan Chase & Co.**, Case # 1:13-cv-03777, Kirkland & Ellis, United States District Court, Southern District of New York. (Patent Non-infringement).
 - Expert Testimony at deposition, Baltimore, MD (June 1, 2017).
- Nader AsghariKamrani and Kamran AsghariKamrani vs. **United Services Automobile Association**. Case # 2:15-CV-478, Fish & Richardson, United States District Court, Eastern District of Virginia. (Patent Written Description Support related to Inequitable Conduct).
 - Expert Testimony **at trial**, Norfolk, VA (April 21, 2017).
 - Expert Testimony at deposition, Baltimore, MD (March 21, 2017).
- **Sabre GBL Inc**, vs. HP Enterprise Services LLC. Case # 1310022761, JAMS Binding Arbitration Hearing, Dallas, TX (Contract dispute).
 - Expert Testimony at arbitration hearing, Dallas, TX (April 5, 2017).
- **Al Cioffi et. al.** vs. Google, Case # 2:13cv103JRGRSP, Vasquez, Benisek & Lindgren, United States District Court, Eastern District of Texas. (patent Infringement).
 - Expert Testimony **at trial**, Marshall, TX (February 7, 2016).
 - Expert Testimony at deposition, Baltimore, MD (September 26, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 14, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2016-00151, Morrison & Foerster, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 19, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01974, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 2, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-02001 & IPR 2016-00157, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 26 & 27, 2016).
- **Amazon.com, Inc** vs. Zitovault, LLC, IPR 2016-00021, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 22, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (May 20, 2016).
- Vir2us Inc. v. **Invincea, Inc. and Invincea Labs, LLC**, Case # 2:15-cv-l62; Cooley, United States District Court, Eastern District of Virginia. (Patent Non-infringement and Invalidity)
 - Expert Testimony at deposition, Reston, VA (April 20, 2016).
- TVIIM. v. **McAfee Inc.**, Case # 3:13-cv-04545-VC; Wilmer Hale, United States District Court, District of N. California. (Patent Non-infringement and Invalidity)
 - Expert Testimony **at trial**, San Francisco, CA (July, 2015).
 - Expert Testimony at deposition, Baltimore, MD (February, 2015).
- Intellectual Ventures vs. **Symantec**, Case # 1:10-cv-01067-LPS; Latham & Watkins, United States District Court, District of Delaware. (Patent Invalidity)
 - Expert Testimony **at trial**, Wilmington, DE (February, 2015).

- Expert Testimony at deposition, Baltimore, MD (May, 2013).
- **Rovi Solutions & Veracode** vs. Appthority, Case # 1210487-DPW; Goodwin Procter, United States District Court, District of Massachusetts. (Patent Infringement and Validity)
 - Expert Testimony at trial, Boston, MA (August 11, 2014).
 - Expert Testimony at deposition, Baltimore, MD (April 4, 2014).
- **Juniper** vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR; Irell & Manella, United States District Court, District of Delaware. (Patent Infringement)
 - Expert Testimony at trial, Wilmington, DE (February, 2014).
 - Expert Testimony in court hearing, Wilmington, DE (November 14, 2013).
 - Expert Testimony at deposition, Baltimore, MD (June, 2013).
- Prism Technologies. v. **Adobe Systems Inc.**, Case # 8:10-cv-00220-LEST-DT; DLA Piper, United States District Court, District of Nebraska. (Patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August, 2012).
- Finjan Inc. vs. **McAfee, Inc.**, Case # 10593 (GSM), Kirkland & Ellis, United States District Court, District of Delaware. (Patent Non-infringement)
 - Expert Testimony at deposition, Washington, DC (June, 2012).
- Avaya Inc. vs. **Telecom Labs Inc., TeamTLI.com Corp., and Continuant Technologies**, Case # 3:06-cv-02490 (GEB); K&L Gates, United States District Court, District of New Jersey. (Contract Dispute)
 - Expert Testimony at deposition, Newark, NJ (August, 2011).
- **Lear Automotive** vs. Johnson Controls Inc (JCI), Case # 04-CV-73461; Flachsbart & Greenspoon, United States District Court, Eastern District of Michigan. (Patent Infringement and Validity)
 - Expert Testimony at trial, Detroit, MI (February, 2011).
 - Expert Testimony at deposition, Baltimore, MD (December, 2005).
- **TecSec Inc** vs. International Business Machines Corporation, Case # 1:10-CV-115-LMB/TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement)
 - Expert Testimony at deposition, Newark, NJ (November, 2010).
- **Echostar Satellite Corporation** vs. NDS Group, Case # SA-CV-03950-DOC(JTL); T. Wade Welch & Associates, United States District Court, Central District of California. (Copyright and DMCA)
 - Expert Testimony at trial, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Baltimore, MD (October, 2007).
- **Web.com Inc** vs. The Go Daddy Group Inc., Case # CV-0701552-PHX-MHM; Graves Law Office, United States District Court, Arizona. (Patent Infringement)
 - Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
 - Expert Testimony at deposition, Baltimore, MD (May, 2008).
- z4 Technologies vs. **Microsoft & Autodesk**, Case # 2:04-CV-00335-LED; Fish & Richardson, United States District Court, Eastern District of Texas. (Patent Non-Infringement and Invalidity)
 - Expert Testimony at trial, Tyler, TX, (April, 2006).
 - Expert Testimony at deposition, Washington DC (January, 2006).

- **Linda Schade** vs. Linda Lamone et. al., Trial on the Legality of Paperless Voting Machines in Maryland. (Adequacy of Voting Equipment)
- Expert Testimony at trial, Annapolis, MD (August 25, 2004).

Awards

- 2020, **Best Paper Award**, in the category of Mobile & Wireless Computing, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- 2020, **Best Paper Award**, in the category of Image Processing & Multimedia Technology, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- IEEE Computer Society Technical Committee on Security and Privacy, **Distinguished Service Award**, May, 2020.
- **Fulbright Scholar** in Israel at Tel Aviv University, academic year 2010-2011.
- 2009, **Google Research Award**, Securing Medical Records on Smartphones.
- Chosen as one of **54 favorite people, places and things in Jewish Baltimore**, Baltimore Jewish Times, February 22, 2008.
- 2007 **Award for Outstanding Research in Privacy Enhancing Technologies**, for Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2005 **Best Student Paper Award** at the 14th USENIX Security Symposium, Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2004 Electronic Frontiers Foundation **Pioneer Award**.
- **Baltimorean of the Year**, Baltimore Magazine, January, 2004.
- 2001 Index on Censorship **Freedom of Expression Award** for the Best Circumvention of Censorship for the Publius project.
- 2000 **Best Paper Award** at the 9th USENIX Security Symposium, A robust, tamper-evident and censorship-resistant web publishing system (with Marc Waldman and Lorrie Cranor).
- 1999 **Best Paper Award & Best Student Paper Award** at the 8th USENIX Security Symposium, The Design and Analysis of Graphical Passwords (with Ian Jermyn, Alain Mayer, Fabian Monrose, and Michael K. Reiter).
- 1996 Coauthor of **Best Student Paper**, Building Systems that Flexibly Control Downloaded Executable Content, at the 6th USENIX UNIX Security Symposium. Student: Trent Jaeger.
- 1992 National Science Foundation **Fellowship Summer Institute in Japan**
- 1986 **Branstrom Prize**, University of Michigan