

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2024-00213
Patent 9,338,140

EXHIBIT 2003

DECLARATION OF AVIEL D. RUBIN, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS	1
III. BASES OF OPINIONS	6
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 1-10)	14
VI. OPINIONS.....	14
A. Petitioner’s Ophir and Takeda Grounds Fail (All Claims, Grounds 1-3).	14
1. The ’140, Ophir, and Takeda.	14
2. A “Plurality Of Shares” “Stored On” “A Plurality Of Physical Storage Devices” (Limitations 1[a], 1[b][2]).....	17
3. Motivation To Combine Ophir And Takeda.	29
4. “A Directory Mapped To The Plurality Of Physical Storage Devices.” (Limitation 1[b][1])	37
B. Petitioner’s Dickinson-Takeda Ground Fails (All Claims, Ground 4).	44
1. The ’140 And Dickinson.....	44
2. Dickinson And Petitioner’s Arguments Were Expressly Considered By The Examiner In Prosecution	56
3. “A Secure Storage System Configured To:” “Present To A Client Device A Virtual Disk, The Virtual Disk Comprising A Directory Mapped To The Plurality Of Physical Storage	

Devices Such That Physical Locations Of The Shares Are Hidden From The Client Device” (Limitation 1[b][1]).	59
a. Dickinson Does Not Disclose Or Render Obvious “A Directory.”	59
b. Dickinson Does Not Disclose Or Render Obvious A Directory “Mapped To The Plurality Of Physical Storage Devices.”	59
c. Dickinson Does Not Disclose Or Render Obvious “That Physical Locations Of The Shares Are Hidden From the Client Device.”	63
d. Dickinson Does Not Disclose Or Render Obvious “A Secure Storage System Configured To: “Present To A Client Device A Virtual Disk.”	67
4. “Plurality Of Shares” “Associated With At Least One Session Key Used To Secure A Dataset” (Limitation 1[a]) “Include With Each Of The Plurality Of Shares Data Indicative Of The At Least One Session Key” (Limitation 1[b][3]).	73
VII. CONCLUSION	78

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. 9,338,140 (“the ’140 patent”) in IPR2024-00213. I have been retained by Security First Innovations, LLC (“SFI”), the Patent Owner in the above proceedings. Petitioner is Google LLC. (“Google” 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. 9,338,140 (Ex. 1001) (“the ’140 patent” or “’140”);
- ii. The prosecution history of the ’140 Patent (Ex. 1002)

- iii. The Declaration signed by Samrat Bhattacharjee, Ph.D. in IPR2024-00213 (Ex. 1003) (the “Bhattacharjee Declaration”);
- iv. The Curriculum Vitae of Samrat Bhattacharjee, Ph.D. (Ex. 1004)
- v. The Petition by Google in IPR2024-00213;
- vi. U.S. Patent Application Publication 2001/022322A2 (“Dickinson”) (Ex. 1005);
- vii. U.S. Patent Application Publication 2004/0143733A1 (“Ophir”) (Ex. 1007);
- viii. U.S. Patent Application Publication 2001/0053221A1 (“Takeda”) (Ex. 1008);
- ix. U.S. Patent No. 7,187,771 (Ex. 1009);
- x. U.S. Patent No. 7,571,320 (Ex. 1010);
- xi. European Patent Application Publication EP 1 063 811 B1 (Ex. 1011);
- xii. U.S. Patent No. 6,151,659 (Ex. 1012);
- xiii. U.S. Patent No. 5,526,507 (Ex. 1013);
- xiv. U.S. Patent No. 6,065,096 (Ex. 1014);
- xv. U.S. Patent No. 7,941,695 (Ex. 1015);
- xvi. U.S. Patent No. 8,352,518 (Ex. 1016);
- xvii. U.S. Patent Application Publication 2002/0174295A1 (Ex. 1017);
- xviii. U.S. Patent Application Publication 2002/0019908A1 (Ex. 1018);

- xix. U.S. Patent No. 7,043,614 (Ex. 1019);
- xx. U.S. Patent No. 6,973,455 (Ex. 1020);
- xxi. U.S. Patent No. 6,697,846 (Ex. 1021);
- xxii. U.S. Patent No. 6,324,648 (Ex. 1022);
- xxiii. U.S. Patent Application Publication 2002/0019932A1 (Ex. 1023);
- xxiv. U.S. Patent No. 5,825,890 (Ex. 1024);
- xxv. U.S. Patent Application Publication 2003/0028493A1 (Ex. 1027);
- xxvi. U.S. Patent Application Publication 2002/0042859A1 (Ex. 1028);
- xxvii. U.S. Patent Application Publication 2005/0216754A1 (Ex. 1029);
- xxviii. U.S. Patent Application Publication 2003/0191938A1 (Ex. 1030);
- xxix. U.S. Patent Application Publication 2003/0167408A1 (Ex. 1031);
- xxx. U.S. Patent No. 7,529,834 (Ex. 1033);
- xxxi. U.S. Patent No. 5,483,598 (Ex. 1034);
- xxxii. Merriam Webster's Collegiate Dictionary, 207, 381, 888 (10th ed. 1997) (Ex. 1037);
- xxxiii. U.S. Patent No. 6,356,915 (Ex. 1038);
- xxxiv. U.S. Patent No. 4,067,058 (Ex. 1039);
- xxxv. Redline Comparison of International Application Publication WO 2001/022322 to U.S. Patent No. 9,338,140 (Ex. 1040);

xxxvi. Google LLC's Proposed Claim Terms for Construction in *Security First Innovations, LLC v. Google, LLC*, 2:23-cv-00097-JWK-RJK (Nov. 11, 2023) (Ex. 1041);

xxxvii. Letter from A. Mayron to D. Perlson re Preliminary Proposed Constructions in *Security First Innovations, LLC v. Google, LLC*, 2:23-cv-00097-JWK-RJK (Nov. 11, 2023) (Ex. 1042);

xxxviii. Microsoft Computer Dictionary, 99, 192, 362, 407 (5th ed. 2002) (Ex. 1043);

xxxix. Security First Innovation's 2023-08-14 Infringement Contentions, Chart D in *Security First Innovations, LLC v. Google LLC*, 2-23-cv-00097 (E.D. Va.) (Ex. 1044);

xl. 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 (September 16, 2005) of the provisional application from which the '140 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 ’140 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. Bhattacharjee has asserted in his declaration that a person of ordinary skill in the art as of the time of the ’140 patent would have had:

at least a bachelor’s degree in computer science, computer engineering, or a related field, with three (3) years of experience in the area of securing data from unauthorized use or access. A higher level of education may substitute for less experience.

Ex. 1003 [Bhattacharjee] ¶ 40.

20. For the purposes of this declaration, I accept Dr. Bhattacharjee'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. Bhattacharjee 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 '140 patent.

B. My Understanding Of Legal Standards

22. When considering the '140 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 1-10)

32. I understand that Petitioner has challenged independent claim 1 and its dependents based on obviousness over Ophir and Takeda (Grounds 1-3) and obviousness over Dickinson and Takeda (Ground 4).

VI. OPINIONS

A. Petitioner's Ophir and Takeda Grounds Fail (All Claims, Grounds 1-3).

1. The '140, Ophir, and Takeda.

33. I understand that Petitioner's first three grounds argue that the claims are disclosed and/or rendered obvious by a combination of Ophir and Takeda. Pet., 2. In my opinion, Ophir and Takeda, however, are both fundamentally different inventions from the '140 and have nothing to do with storing file shares separately in different physical locations as the '140 does.

34. The '140 is directed towards an "ever-increasing need" to ensure stored data cannot be read or otherwise compromised by unauthorized parties. Ex. 1001 ['140] 1:22-29. To address this need, the '140 "provide[s] a method for securing virtually any type of data from unauthorized access or use" which includes, first, "parsing, splitting and/or separating the data to be secured into two or more parts or portions," identified as shares. *Id.*, 2:33-37.

35. The '140 then teaches the significant security advantages derived from storing those shares amongst multiple physical storage devices, which I discuss later.

36. The '140's claimed inventions, and related disclosure, concern a "secure storage network" for storing a dataset provided by a client system, where the dataset is divided into a plurality of "shares" and further secured using a "session key." Ex. 1001 ['140] 98:2-22; 87:15-59. The claims further require including with each of the plurality of "shares" "data indicative of the at least one session key used to secure the dataset." *Id.*, 98:2-22; 55:56-56:41.

37. The claims additionally require a directory, mapped to a plurality of physical storage devices, to manage the shares associated with a given dataset. Ex. 1001 ['140] 98:2-22; 87:16-34. The directory provides client systems with a view of stored datasets but hides the underlying distribution of the shares among the storage devices from the client device. *Id.*, 87:35-59. In this way, an interface is provided that allows client systems to access the entirety of a particular dataset without knowledge of the location of its individual shares. This enhances security by reducing the likelihood that an attacker with access to a client system can gain access to enough shares to reconstitute a dataset.

38. The claimed system provides enhanced security for the dataset because the shares (along with information regarding the session key) are stored on

a plurality of storage devices located in different physical locations, such that an attacker cannot reconstruct the dataset without access to at least a portion of the separately stored shares. *Id.*, 55:56-56:3. The claims relate to the '140's teachings concerning a distributed file system that incorporates a directory to manage the shares associated with a given dataset. *Id.*, 87:16-34. The directory provides client systems with a view of stored datasets but hides the underlying distribution of the shares among the storage devices. *Id.*, 87:35-59. In this way, an interface is provided that allows client systems to access a particular dataset without knowledge of the location of its individual shares. This enhances security by reducing the likelihood that a client system, or an attacker with access to a client system, can gain access to enough shares to reconstitute a dataset without authorization.

39. Ophir discloses a “mediator” that provides an interface between networked storage devices and client devices using a variety of protocols. “The mediator functions as a central point” for the encryption of datasets from the data clients to be stored on the storage devices, as well as decryption of the encrypted dataset retrieved from the storage devices for delivery to the data clients. Ex. 1007 [Ophir] Abstract. The mediator makes storage available for datasets provided by the clients, without requiring the clients to be involved in encryption or decryption operations, or burdened with key management. *Id.* Nothing in Ophir indicates that

the mediator divides the datasets into shares, or stores a particular dataset on more than one storage device.

40. Takeda discloses a “ciphering apparatus” in which a plaintext dataset provided by a client is divided into blocks and the blocks are individually encrypted. Ex. 1008 [Takeda] Abstract. All of the separately-encrypted blocks are stored together in a single file on a single storage device, either with or without information about the keys or other techniques used to encrypt them. *See, e.g.*, Ex. 1008 [Takeda] ¶56.

41. Thus, in contrast to the ’140, neither Ophir nor Takeda concern dividing a dataset into shares **and** storing those shares amongst multiple storage devices.

2. A “Plurality Of Shares” “Stored On” “A Plurality Of Physical Storage Devices” (Limitations 1[a], 1[b][2]).

42. Claim 1 requires:

Limitation 1[a] “a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset;”

Limitation 1[b][2] “generat[ing]the plurality of shares ... by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares.”

43. Limitations 1[a] and 1[b][2] require a “plurality of shares,” *i.e.*, two or more shares be stored on a “plurality of physical storage devices,” *i.e.*, two or more storage devices.

44. These limitations reflect the ’140’s teachings that distributing shares amongst multiple storage devices substantially increases the security of sensitive information. Ex. 1001 [’140] 95:15-18 (“The sensitive information 5404, 5406, 5408 may be parsed and distributed to multiple locations...”); 21:4-12 (“the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities ... such that no single data storage facility ... includes sufficient encrypted data to recreate the original sensitive data S”); 69:16-22 (“if each of four portions is stored in a different physical location ... then, if ... two of the locations may be compromised whereby data is destroyed or inaccessible ... the original data may still be retrieved from the portions in the other two locations.”); 53:6-18 (describing four methodologies, each of which disperses dataset shares amongst “multiple locations”); 56:37-40 (Figure 21 embodiment stores shares/keys in “different locations”); 58:64-59:6 (“shares” “a” and “b” are “placed in separate depositories”); 60:43-51 (“When the shares of data are split physically and under the control of different personnel, for example, the possibility of compromising the data is greatly reduced.”); 96:6-9 (“a backup of the files is parsed to multiple backup locations in accordance with the present invention.”);

59:27-34 (storing shares in different depositories); 83:12-30 (discussing storing shares at different sites).

45. Furthermore, I note the Examiner (in prosecution) and the parties here have uniformly recognized that the claims require storing shares on different physical storage devices.

46. The prosecution history, consistent with the plain meaning of the claims, reinforces the requirement that the plurality of shares be stored on two or more storage devices. There, the Examiner found that limitation 1[a]’s requirement of “a plurality of physical storage devices” was allegedly satisfied by Dickinson’s disclosure of data storage facilities D1, D2, D3, and D4 and the requirement of “storing thereon a plurality of shares” was allegedly taught by a disclosure that “the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S.” See Ex. 1002 [Pros.-Hist.] 1236-1237 (quoting Ex. 1005 [Dickinson] 21:10-14).

47. This understanding of the claim is also undisputed by the parties. Petitioner contends that Dickinson meets limitation 1[a] because the “encryption results (‘B’ and ‘D’) [are stored] **on at least two** of storage devices D1-D4.” Pet., 68. Similarly, in district court, Patent Owner’s infringement contentions rely on

Petitioner's storage system being designed such that "the dataset is broken up into shares for storage" and "'**will not be stored entirely in a single server**, but instead will be broken up into chunks' and **stored across different servers.**" Ex. 1044 [PO-Infringement-Contentions] 34.

48. Thus, the plain meaning of the claims, the specification, and the prosecution history are consistent in requiring that a dataset be divided into two or more shares which must be stored on two or more storage devices. There is further no dispute between the parties that the claims require that the two or more shares must be stored on two or more storage devices. The claim limitations are not satisfied if the plurality of shares are generated, but only stored on a single storage device.

49. I note that neither Ophir nor Takeda suggest storing shares of a given dataset on different storage devices. Petitioner and Dr. Bhattacharjee contend Takeda's blocks comprise a "plurality of shares" and that these shares would be stored on Ophir's "plurality of storage devices": "Ophir-Takeda stores the plurality of shares [Takeda's ciphered blocks] on [Ophir's] plurality of storage devices." Pet., 31.

50. First, Petitioner and Dr. Bhattacharjee argue that Takeda teaches a "plurality of shares" for the limitation-at-issue because:

Ophir-Takeda implements Takeda’s ciphering technique, which divides received data into a plurality of blocks Mn. ...

In Ophir-Takeda, each data block Mn is ciphered using a respective cipher attribute An (which may include a ciphering key—Takeda, [0042]) to form a ciphered block Cn. Takeda, FIGs. 2B, 11B-11D [sic], [0040]-[0042], [0068]; §§VII.B, VII.C.3 *supra*; Bhattacharjee, ¶107.

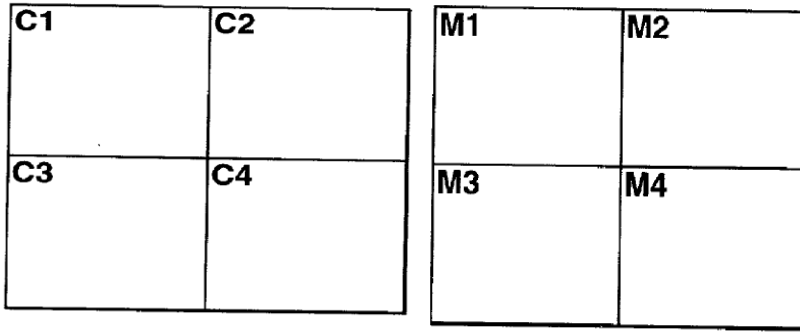


FIG.2B

FIG.1B

Each ciphered block (Cn) is a “share” as claimed because it is a portion of the ciphered (i.e., encrypted) dataset, which the ’140 patent’s specification calls a “share.” EX1001, 53:19-28 (equating “share” and “portion”), 55:59-66 (discussing “storing the shares” after each “portion[]” is encrypted); 56:25-27 (“[s]eparating...encrypted data” results in “shares or portions of parsed data”), 56:60-62, 57:36-38, 58:11-13; *see also* EX1001, 59:15-18 (describing encrypted data “segments” as “shares”); Bhattacharjee, ¶108. Ciphertext block (Cn) together with its corresponding key (“ciphering attribute” An)

(Takeda, FIG. 3A) meet a “share” as claimed if the share is construed to require storing information linking the share to the key that is used to secure the share. Bhattacharjee, ¶108. Each ciphertext block (C_n) together with a pointer to its corresponding key (“ciphering attribute” A_n) is a “share” as claimed if a “share” is construed to require storing information linking the share to the key used to secure it. (Takeda, [0040]); Bhattacharjee, ¶108.

Pet., 28-29. I note that Takeda classifies its divided dataset as “blocks” rather than “shares,” and that neither Petitioner nor Dr. Bhattacharjee point to a disclosure in Takeda wherein the blocks are distributed to more than one physical storage device. Instead, it appears that Takeda’s blocks are stored together in a single storage device.

51. Even assuming that Takeda’s blocks are “shares,” Takeda does not teach or suggest storing its blocks/shares on two or more physical storage devices. Rather, Takeda’s encrypted blocks (aka “ciphertext”) are all stored in a single place (*e.g.*, “storage device 37” or “removable recording medium 39”). Ex. 1008 [Takeda] ¶¶91-92 (“The ciphertext is stored in the removable recording medium 39 or the storage device 37”), ¶¶7-8 (encrypted blocks are ciphertext).

52. Takeda does not teach storing two or more blocks of a dataset on two or more physical storage devices. Instead, Takeda suggests the opposite, indicating that its blocks are stored together. For example, Takeda’s Figures 1B, 2B, 3A, and 3B, below, each show configurations of the divided dataset wherein

the blocks are shown as stored together, both before ciphering (Fig. 1B) and after ciphering (Figs. 2B, 3A, 3B):

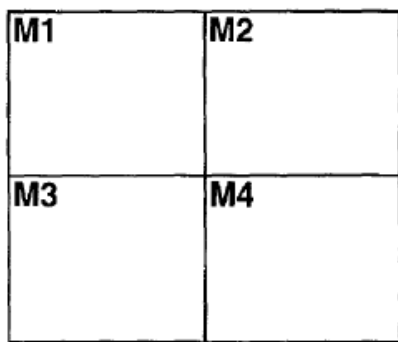


FIG.1B

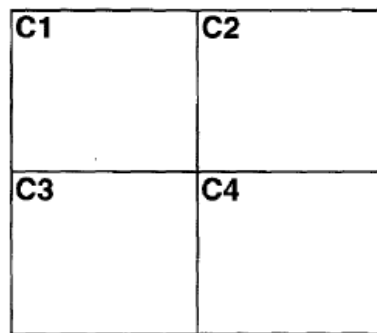


FIG.2B

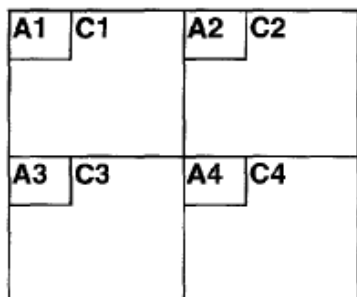


FIG.3A

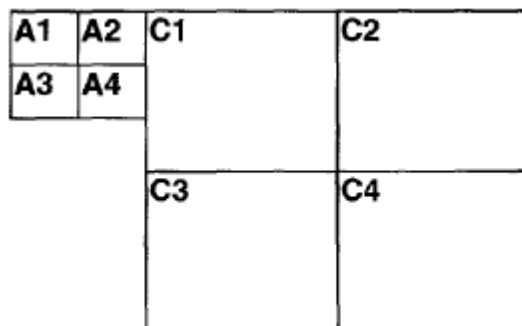


FIG.3B

53. This accords with Takeda’s written description which refers to the ciphered blocks collectively as a “ciphertext data group.” *Id.*, ¶48.

54. I understand that Petitioner and Dr. Bhattacharjee argue that Ophir discloses “a plurality of physical storage devices” for the limitation-at-issue, because:

Ophir's "[s]torage devices...encompass various devices known in the art, including, but not limited to: mainframe storage; SAN-in-a-box; simple RAID; NAS filer; iSCSI storage; tape library; optical juke box; and JBOD ('Just a Bunch Of Disks'), which herein denotes any collection of one or more disk drives which does not necessarily include any special coordinating controller or data processing." Ophir, [0034] (discussing FIG. 7, excerpted below, illustrating "representative...technologies...which can be utilized by" Ophir's "invention"):

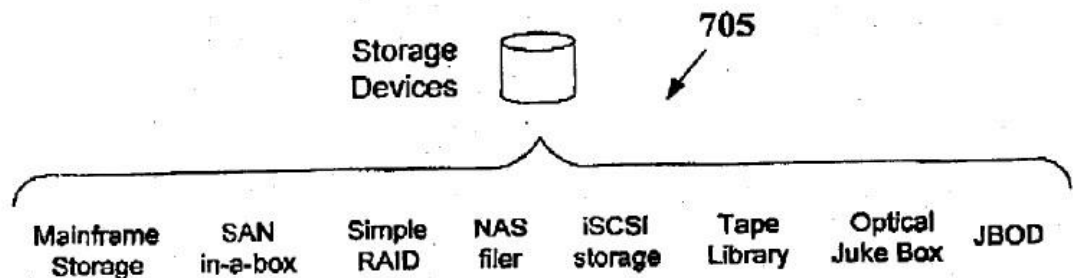


FIG. 7.

POSAs understood these are all examples of physical storage devices, at least some of which (e.g., JBOD, RAID) include a plurality of devices. Bhattacharjee, ¶¶99-105 (citing, e.g., EX1012, 1:4-6, 1:13-17; EX1013, 1:57-63; EX1014, 1:25-27 regarding RAID).

Pet., 27. Notably, however, while Petitioner points to a disclosure in Ophir for multiple storage devices, Petitioner does not point to a disclosure of storing parts or portions of a single dataset on two or more physical storage devices.

55. Ophir concerns a secure storage network with a “secure storage data mediator” that receives and stores information from multiple clients across multiple storage devices. Ex. 1007 [Ophir] ¶¶11-13, Fig. 4. Ophir’s goal is to provide a storage network that “offers both the flexibility, expandability and scalability of [a] network, but which also places no encryption burdens on the data clients.” *Id.*, ¶8; *see also id.*, ¶¶9, 15.

56. But Ophir does **not** disclose or suggest, at all, dividing a dataset into pieces or anything else that might correspond to the “shares” of claim 1, much less storing those pieces on two or more physical storage devices.

57. I have been informed and understand that in single-reference obviousness, when a missing limitation goes to the heart of an invention, review of any purported reasoned basis for resort to common sense must be especially searching. Moreover, common sense used to supply a missing limitation can be used only when the missing limitation is unusually simple and the technology particularly straightforward.

58. Here, the limitation is of crucial importance to the claimed invention and is neither unusually simple nor particularly straightforward. As I previously discussed, the ’140 teaches that dividing a dataset into shares and storing those shares across multiple storage devices significantly enhances both the security and recovery of stored data. Similarly, the field of data security is quite complicated

and intricate. The inventions-at-issue concern cryptography, which is a technologically-involved and complex field involving incredibly high stakes and safeguarding against a wide variety of highly sophisticated and ever-evolving cybersecurity attacks. As internationally-renowned cryptologist Bruce Schneier (Ex. 2005 [Schneier-CV]) has observed “[f]ew can do the science [of cryptography] properly” and “[g]ood cryptographers know that nothing substitutes for extensive peer review and years of analysis.” Ex. 2006 [Schneier-Why-Cryptography-Is-Harder-Than-It-Looks] 3.

59. Petitioner fails to demonstrate that a POSITA would be motivated to combine Ophir and Takeda such that Takeda’s blocks are stored amongst multiple storage devices. Petitioner posits implementing Takeda’s block-based encryption scheme in conjunction with Ophir’s mediator. *See* Pet., 17 (“A POSA would have been motivated by Takeda to implement Takeda’s ciphering/deciphering as the encryption/decryption performed by Ophir’s encryption/decryption unit (*e.g.*, encryption/decryption unit 517) to achieve ‘a more reliable ciphering technique’ as taught by Takeda.”). Petitioner contends that, “[b]esides modifying Ophir’s encryption/decryption techniques to use those of Takeda, Ophir-Takeda need not change Ophir’s other aspects.” *Id.*, 25.

60. Thus, Petitioner’s combination is focused upon implementing Takeda’s block-based scheme in Ophir’s system. In other words, Petitioner

contends that a POSITA would replace Ophir's encryption scheme, in which a file is encrypted and then stored on one of several available storage devices, with Takeda's scheme, in which the blocks of a file are separately encrypted and stored together in a single file on a storage device.

61. What is missing is any indication or argument that, even with that replacement, a POSITA would be motivated to divide Takeda's blocks from a given dataset across two or more of Ophir's physical storage devices. That was the inventors' insight, and Petitioner's argument to the contrary is pure hindsight.

62. Petitioner does not account for this gap as it merely asserts that the "Ophir-Takeda" combination "stores the plurality of shares ... on the system's plurality of storage devices." Pet., 31. Nor does Petitioner provide any reason for why importing Takeda's ciphering/deciphering scheme into Ophir would naturally result in Takeda's blocks from a given dataset being split up amongst multiple storage devices, as nothing in either reference suggests splitting a dataset and storing different parts of that dataset amongst multiple storage devices.

63. I note that Petitioner and Dr. Bhattacharjee do not offer any reason why a POSITA would combine Ophir-Takeda such that this dispersed storing would be implemented, nor do they demonstrate that such storing would be a natural by-product of the combination. I further do not see any demonstration from Petitioner or Dr. Bhattacharjee that such storing would be a natural by-

product of the combination. *See* Pet., 31 (“Ophir-Takeda stores the plurality of shares ... on the system’s plurality of storage devices” because “Takeda’s ciphering is performed in Ophir’s ‘Encryption/Decryption Unit’ 517 ... and the encrypted shares are stored on the above-discussed plurality of storage devices.”). Consequently, in my opinion, Petitioner and Dr. Bhattacharjee’s analysis is conclusory and insufficient.

64. In essence, Petitioner and Dr. Bhattacharjee rely upon two references, one with multiple alleged data shares (Takeda) and one with multiple storage devices (Ophir). Neither reference, however, discloses or suggests dividing a dataset into shares and storing those shares amongst multiple physical storage devices. While dividing a dataset into blocks may have been known, and having a system with multiple storage devices may also have been known, that does not establish that it would be obvious to divide a dataset into shares and store those shares across physically distinct storage devices. The innovation described in the ’140 is a central insight of the inventors, one that is taught at length to secure data, and not taught or suggested by either Ophir or Takeda.

65. Thus, in my opinion, Petitioner and Dr. Bhattacharjee fail to demonstrate that a combination of Ophir and Takeda disclose or renders obvious either “a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure

a dataset” or “generat[ing]the plurality of shares ... by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares.”

3. Motivation To Combine Ophir And Takeda.

66. Petitioner proposes implementing Takeda’s block-based ciphering/deciphering techniques in Ophir’s system:

Implementing Takeda’s ciphering/deciphering technique in Ophir’s encryption/decryption unit 517 is a simple substitution of Takeda’s known encryption/decryption technique for Ophir’s encryption/decryption technique. Bhattacharjee, ¶90. This can be done by substituting Takeda’s FIG. 19 ciphering apparatus 10 for Ophir’s encryption unit 513 and Takeda’s FIG. 20 deciphering apparatus 20 for Ophir’s decryption unit 515, or adapting/programming Ophir’s units to perform Takeda’s techniques. Bhattacharjee, ¶90. For example, Takeda’s ciphering apparatus 10 and Ophir’s encryption unit 513 both take in data to be ciphered (i.e., encrypted) and output ciphered data. Takeda, [0088]; Ophir, [0032]; Bhattacharjee, ¶90; *see also* EX1010, 1:35-41 (ciphering engine produces encrypted data output); EX1011, [0002] (“cryptographic algorithms, also known as ciphers” are used “to encrypt data”). Similarly, Takeda’s deciphering apparatus 20 and Ophir’s decryption unit 515 both take in ciphered data and output deciphered (i.e., decrypted) data. Takeda, [0090] (Takeda’s “ciphertext and attribute table input section” 21 receives “ciphertext” which is the ciphered

data along with the attribute table and outputs “plaintext” which is deciphered data); Bhattacharjee, ¶90.

Pet., 21. In my opinion, however, a POSITA would not be motivated to make this combination. Ophir is directed towards achieving a network that can securely store datasets from multiple clients, **without** requiring anything from the client to secure the dataset. See Ex. 1007 [Ophir] ¶8 (Ophir’s goal is to provide “a network system for secure data storage ... which ... places no encryption burdens on the data clients”); *id.*, ¶¶5, 7 (similar). But adding Takeda’s block encryption system would do the opposite, by requiring the data clients to be intimately involved in Ophir’s data encryption. Thus, such a modification would be contrary to Ophir’s goals and principle of operation.

67. Ophir is directed towards a networked data security system which can safely store data for multiple clients without putting any burdens on those clients relating to securing the data. Ophir expressly seeks to improve upon prior art data systems that “require[d] data clients to perform procedures related to critical cryptographic operations necessary for data security,” which “puts stringent limitations on the ability of the system to optimize encryption methods and keys.” Ex. 1007 [Ophir] ¶7. Ophir, thus, explains that there is “a need for, and it would be highly advantageous to have, a network system for secure data storage which offers both the flexibility, expandability, and scalability of the network, but **which**

also places no encryption burdens on the data clients.” *Id.*, ¶8. Ophir further explains that this “goal is met by the present invention.” *Id.*

68. Consistent with this objective, Ophir’s “Summary of the Invention” explains that “[i]t is an objective of the present invention to provide secure data storage accessible to data clients over a network ***without requiring the data clients to perform any operations related to the security of the stored data***, including, but not limited to, encryption, decryption, key management, key distribution, key storage, and key updating.” *Id.*, ¶9. The system “imposes no requirement for data clients to perform security-related operations,” and any such involvement is purely optional. *Id.*

69. To carry out this objective, Ophir discloses a “secure data storage mediator,” which is not a user, but, rather, an automated entity that acts as a “central coordinator for data storage” (Ex. 1007 [Ophir] ¶13), that facilitates the encryption/decryption such that “data clients do not have to be involved in any aspects of the encryption/decryption of data in storage.” *Id.*, ¶15. Ophir confirms that “[t]he novel aspects of the present invention lie in the protection of data for storage, which the mediator performs over the network without imposing ***any*** compulsory involvement of the data clients.” *Id.*; see also *id.*, ¶28 (“In the case of the prior-art ***requirement for data clients to participate*** in the encryption and/or

decryption processes, the ***lack of such a requirement*** by the present invention is a ***clear-cut advantage.***”).

70. Thus, the problem Ophir is trying to solve, its goal, and the novel aspect of its system is to have a networked data storage system that “places no encryption burdens on the data clients” (*id.*, ¶8), does not “requir[e] the data clients to perform any operations related to the security of the stored data” (*id.*, ¶9), and ensures that data is securely stored “without imposing ***any*** compulsory involvement of the data clients” (*id.*, ¶15).

71. Ophir’s goal and principle of operation, wherein no encryption burden is placed on data clients, is thwarted by the addition of Takeda’s ciphering/deciphering techniques, wherein user involvement, vis-à-vis a client device, is required.

72. Adding Takeda’s ciphering/deciphering techniques to Ophir’s system would be entirely contrary to Ophir’s goal and principle of operation because Takeda’s methodology ***requires*** the data clients (Takeda’s “users”) to be heavily involved in the ciphering/deciphering processes.

73. Takeda’s ciphering/deciphering processes requires user involvement at multiple stages, including providing or determining a ciphering attribute (*e.g.*, a “ciphering key[]” or “algorithm[] for ciphering” per Takeda, ¶42) for each block into which the data set is divided, and when/whether to continue or end the

ciphering/deciphering processes. Takeda makes clear that the user determines, inputs, and sets the ciphering attribute, and does not disclose any alternative to the user's involvement. Ex. 1008 [Takeda] ¶9 (“**a user** appropriately **determines the ciphering attribute**”), ¶56 (“a **user** who wishes to cipher the plaintext **inputs the attribute**”), ¶88 (“the **user sets the attribute** for each block”), Fig. 19 (illustrating user input in ciphering). Takeda's user also determines whether the ciphering/deciphering processes should continue or terminate. Ex. 1008 [Takeda] ¶56 (user must “input whether or not the ciphering processing is to be ended”), Fig. 5 (illustrating user input in ciphering process), ¶58 (“... the **user** ... instruct[s] whether or not to end the deciphering process.”), Figs. 5-6 (illustrating user input in deciphering process). Petitioner recognizes that the data clients are intimately involved in Takeda's encryption operations, noting that “[t]he user sets the attribute for each block using attribute setting section 12...” Pet., 15.

74. Thus, contrary to Ophir's goal, Takeda **requires** user involvement throughout the ciphering/deciphering process. While Takeda discusses a user (usually a person) rather than a data client (usually a computer), the user's involvement would be manifested through computers (data clients) and further introduces the additional element of human error.

75. Thus, introducing Takeda's encryption/decryption process in Ophir's system would be entirely contrary to Ophir's goals and principle of operation.

Whereas Ophir's entire purpose is to create a networked system that does not require any involvement by the data clients in the encryption/decryption process, particularly for data in storage, Takeda **requires** not only data clients, but the human users thereto, to be intimately involved in key aspects of the ciphering/deciphering process of stored data.

76. I note that Petitioner proposes adding Takeda's techniques to Ophir, **without** changing Takeda's techniques or otherwise modifying Ophir's system. Pet., 21-22 (substitution of Takeda's techniques or apparatuses "would have predictably resulted in Ophir's data ciphering/deciphering ... being performed **as described by Takeda**"), 25 ("Besides modifying Ophir's encryption/decryption techniques to use those of **Takeda**, Ophir-Takeda **need not change Ophir's other aspects.**"). Therefore, in my opinion, Petitioner offers no suggestion that Takeda's ciphering/deciphering techniques would be modified to operate without the necessary involvement of the users/data clients. I do not see any indication that Petitioner even confronts the detrimental effects that adding Takeda's ciphering/deciphering techniques would have with respect to Ophir's goals. Thus, as I addressed above, a POSITA would not be motivated to combine Ophir and Takeda, especially when no changes are made to mitigate the effects that implementing Takeda's techniques would have with respect to Ophir's clearly stated goals.

77. As addressed above, a POSITA would not be motivated to modify Ophir in view of Takeda as Petitioner suggests. Petitioner identifies three purported reasons why a POSITA “would be motivated by Takeda to implement Takeda’s ciphering/deciphering technique (splitting the data into blocks and encrypting different blocks with different ciphering attributes) in Ophir.” Pet., 17-25. None of Petitioner’s proposed motivations address the above-referenced issue. Further, in my opinion, none of these reasons are persuasive because they do not explain why or how a POSITA would modify Ophir to store blocks amongst multiple storage devices, or that a POSITA would have a reasonable expectation of success in doing so.

78. Petitioner contends that a POSITA would modify Ophir by “simpl[y] substitut[ing]” Takeda’s block-based encryption/decryption technique for Ophir’s file-based encryption/decryption technique. Pet., 21. It explains that a POSITA would be motivated to “split[] the data into blocks and encrypt[] different blocks with different ciphering attributes.” *Id.*, 18. A POSITA would be motivated to do so, Petitioner asserts, “to achieve ‘a more reliable ciphering technique’” wherein ““even if a part of the data is deciphered, the rest of the data is not easily deciphered.”” *Id.*, 17 (citing Ex. 1008 [Takeda] ¶6).

79. But the “simple substitution” envisioned by Petitioner (and, as explained, it is neither simple nor even feasible), whatever the reason for it, would

not achieve the claimed invention. Claim 1 requires, in addition to the creation and encryption of shares, that different shares be stored amongst multiple storage devices. But even assuming that “blocks” in Takeda correspond to “shares” in claim 1, Takeda cannot motivate one of skill to modify Ophir to store different shares amongst multiple storage devices because it does not teach or contemplate anything other than storing all of the blocks together in a single file on a single storage device. *See* Ex. 1008 [Takeda] ¶¶48, 91-92, Figs. 1B, 2B, 3A, 3B.

80. Nor would a POSITA have a reasonable expectation of success in achieving the “different blocks on different storage devices” aspect of claim 1 by modifying Ophir in light of Takeda. Takeda does not even teach how a dataset should be divided into blocks, much less how blocks could be identified and tracked on different storage systems in order to permit reconstruction of a data set. *See* Ex. 1008 [Takeda] ¶64 (stating that “[i]n the above description ... a way of forming blocks ... has not particularly been described [but] may be designated by the user or by using a specific algorithm.”). Nor could it since all of Takeda’s blocks from a given dataset are stored together. And the gap is not filled by Ophir itself, because the Ophir mediator only stores files (Ex. 1007 [Ophir] ¶¶12-13), not parts of files, and it discloses no way to track, identify, find or retrieve different blocks stored on different storage devices, as would be required to reconstruct a dataset and provide it to a client device.

81. I do not see any mention, let alone explanation for, Petitioner and Dr. Bhattacharjee's failure of proof.

82. Thus, in my opinion, Petitioner and Dr. Bhattacharjee fail to demonstrate that a POSITA would be motivated to combine Ophir and Takeda in the manner they have described.

4. "A Directory Mapped To The Plurality Of Physical Storage Devices." (Limitation 1[b][1])

83. Claim 1 requires:

Limitation 1[b][1] "present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device."

84. Petitioner argues that Ophir discloses and/or renders obvious this limitation through Ophir's disclosure of: (1) a mediator (Pet., 32-35); (2) block services (Pet., 35-37), or (3) file services. Pet., 37-39.

85. First, Petitioner and Dr. Bhattacharjee contend that:

Because the client can retrieve stored data through the mediator without knowing the data's stored location (Ophir, [0012]-[0013]) (i.e., "physical locations of the shares are hidden from the client device" as claimed (EX1001, 98:10-11)), POSAs would have understood that Ophir maintains a directory mapping where in the physical storage locations each piece of client data is stored, so that

the mediator can retrieve the data when the client desires. Bhattacharjee, ¶117.

Pet., 34; Ex. 1003 [Bhattacharjee] ¶ 117 (same).

86. I do not see any identification from Petitioner or Dr. Bhattacharjee of any express disclosure of a “directory” in Ophir, much less one “mapped to the plurality of physical storage devices.” This is not surprising because Ophir does not disclose how the mediator retrieves data. Ex. 1007 [Ophir] ¶13 (“the mediator is able to store data in, and retrieve data from, any suitable storage device having access to the network.”). I note that Petitioner does not address how Ophir’s mediator would inherently use a “directory mapped to the plurality of physical storage devices” to retrieve requested data. Thus, I see no support for Petitioner’s argument that Ophir’s data retrieval is done through a “directory.”

87. Petitioner alternatively asserts that “maintaining such a directory mapped to the physical storage devices would have been a conventional and obvious way to implement what Ophir describes to allow the mediator to retrieve client data for the data clients when the client does ‘not know the locations where the data is stored.’” Pet., 34 (citing Ex. 1007 [Ophir] ¶13; Ex. 1003 [Bhattacharjee] ¶¶117-119). But I see no explanation by Petitioner why this would be a “conventional and obvious way to implement what Ophir describes.” Thus, I disagree with Petitioner.

88. Second, Petitioner argues that Ophir’s mediator provides “block services,” “which POSAs would have understood means that the mediator provides block-based virtual storage.” Pet., 35. Petitioner further contends that “POSAs would have understood that storage blocks presented to a data client are blocks of a virtual (rather than physical) disk, wherein the virtual disk comprises a directory mapped to the plurality of physical storage devices.” Pet., 36 (citing Ex. 1016, 5:39-58; Ex. 1017, ¶20; Ex. 1018, ¶29, Fig. 16; Ex. 1003 [Bhattacharjee] ¶132). I disagree.

89. I note that Petitioner and Dr. Bhattacharjee again fail to point to any disclosure in Ophir of a “directory” in connection with the disclosed “block services,” much less one “mapped to a plurality of physical storage devices.” The Petition quotes Ophir for the proposition that the mediator provides “virtual secure storage,” suggesting that this corresponds to the “virtual disk” of the ’140’s claim 1. Pet., 9. However, Ophir explicitly states that its storage is considered “virtual” not because it is presented as a single storage device, but only “because the data ... can be stored on a variety of storage devices using a variety of protocols, technologies and services ...” Ex. 1007 [Ophir] ¶33. Petitioner does not point to any disclosure in Ophir of a “directory” in connection with the disclosed “block services.” Petitioner also does not point to any such directory “mapped to a plurality of physical storage devices.” I note Petitioner argues a POSITA would

“understand” that block services entail such a directory, and that what a POSITA would understand requires that Petitioner show that such a directory is inherent in the disclosure. I see no indication that Petitioner has attempted to prove that Ophir’s system necessarily includes a directory mapped to a plurality of physical storage devices. Thus, I am unpersuaded by Petitioner and Dr. Bhattacharjee’s argument.

90. Petitioner alternatively argues a mapping directory “would have been the conventional and obvious way to implement what Ophir describes” because “the mediator provides ‘virtual’ storage, data is accessed by a client on a block level, and the client need not know where the data is physically stored.” Pet., 36 (citing Ex. 1007 [Ophir] ¶¶13, 33; Ex. 1019 1:39-50, 2:13-24; Ex. 1015, Fig. 14A, 7:32-40, 8:55-9:3; Ex. 1016, 2:57-3:3, 5:39-58; Ex. 1017 ¶20; Ex. 1018 ¶¶29, 45-48; Ex. 1003 [Bhattacharjee] ¶133).

91. Petitioner cites to specific excerpts of Exhibits 1015-1019 in support of its proposition that “implementing a virtual disk by using a mapping directory ... would have been the conventional and obvious way to implement what Ophir describes.” But Petitioner fails to show its citations actually teach a “directory mapped to the plurality of physical storage devices.” Some of Petitioner’s citations discuss some form of mapping, but not a directory (Ex. 1017 ¶20; Ex. 1018 ¶¶29, 45-48), another discusses a “directory” but not mapping (Ex. 1016, 2:57-3:3, 5:39-

58), while the remaining two discuss neither (Ex. 1019 1:39-50, 2:13-24; Ex. 1015, Fig. 14A, 7:32-40, 8:55-9:3). Nor does Petitioner expand on how these five separate references should be taken together to modify Ophir such that it would teach this limitation. Petitioner simply has not shown that a directory mapped to a plurality of physical storage devices is a conventional and obvious way of implementing Ophir.

92. I note that Petitioner does not show what motivation a POSITA would have to modify Ophir in the face of its five references, Exhibits 1015-1019, especially because Ophir already performs the recovery task in a different way.

93. Petitioner further contends that implementing a “directory mapped to the plurality of physical storage devices” would be appropriate because “virtual disks were known to use a mapping directory to map virtual storage blocks to physical storage locations.” Pet., 37 (citing Ex. 1007 [Ophir] ¶¶13, 33; Ex. 1003 [Bhattacharjee] ¶¶133-34). But, as discussed, Ophir does not disclose a “virtual disk” in the way the term is used in claim 1.

94. And Petitioner’s citation to Ophir’s ¶¶13 and 33 do not help it. Ophir at ¶13 states:

The mediator is able to receive data from, and transmit data to, any data client having access to the network. Likewise, the mediator is able to store data in, and retrieve data from, any suitable storage device having access to the network. In is manner, the mediator

functions as a central coordinator for data storage between one or more clients requesting data storage and one or more storage devices providing data storage. In this central point, the mediator serves as a virtual secure storage device. The data clients do not have to be involved in any storage or retrieval operation with any storage devices, and need not know the locations where the data is stored. Similarly, the mediator performs encryption and decryption functions to secure the stored data without requiring the data clients to participate in any encryption or decryption on operations related to the security of stored data. (As noted previously, however, participation of the data clients in such encryption and decryption operations is not compulsory, but data clients may optionally perform encryption and/or decryption.) The data clients, for example, do not need to have access to any keys required for the encryption or decryption of stored data. In particular, the mediator is not required to obtain keys from the data clients, and in an embodiment of the present invention, the mediator obtains keys from sources other than a data client.

Ex. 1007 [Ophir] ¶13.

95. Petitioner's other citation, Ophir at ¶33, states:

FIG. 6 illustrates the capacity of a mediator **601** to effort secure virtual data storage for a data client **603** over a network connection **605**. The storage is considered “virtual” because the data from data client **603** can be stored on a variety of storage devices using a variety of protocols, technologies, and services, as managed by mediator **601**. For example, mediator **601** is able to support technologies including, but not limited to a Gigabit Ethernet link **615**, which connects to a

data storage device **617** and a fiber channel **619**, which connects to a data storage device **621** utilizing block device application protocols including, but not limited to, **SCSI** and **iSCSI**, and file system application protocols including, but not limited to, **NFS**. Moreover, mediator **601** is also able to provide block services **623**, file services **625**, and database services **627** (the capabilities for which are contained therein, as illustrated), while providing protocol translation between application protocols used with clients and application protocols used for storage devices and encrypting and decrypting the data that is stored on the storage devices. Additional application protocols include, but are not limited to, FCP (SCSI over FC), CIFS, and iSCSI. The mediator is able to provide block device services, file services, and database services, and is also able to provide encryption of the raw data (e.g., a block device's data, and a file's data).

Ex. 1007 [Ophir] ¶33.

96. Neither Ophir at ¶13 or ¶33 disclose a mapped directory, and thus do not help Petitioner.

97. Third, Petitioner alternatively contends Ophir's disclosure of "file services" discloses and/or renders obvious the "directory" of limitation 1[b][1], claiming that because a client can retrieve files from storage via the mediator, a "directory mapped to the plurality of physical storage devices" must be included as part of Ophir's "file services." See Pet., 38 (citing Ex. 1007 [Ophir] ¶¶46-47; Ex. 1003 [Bhattacharjee] ¶¶137-40). I note that Petitioner points to no express

disclosure in Ophir for this proposition. Petitioner cites to Ophir at ¶¶46-47 for such knowledge, but these citations do not mention a directory or the required mapping.

98. Petitioner alternatively argues “maintaining a ‘directory’ mapped to the physical storage locations would have been a conventional and obvious way to implement Ophir’s file system because a file system conventionally maintains such directories.” Pet., 39. But Petitioner and Dr. Bhattacharjee fail to explain what benefits the modification would render, what changes must be made to Ophir’s system, or what success a POSITA would have making such a modification.

99. Thus, in my opinion, Petitioner and Dr. Bhattacharjee fail to demonstrate that a combination of Ophir and Takeda would disclose or render obvious “a directory mapped to the plurality of physical storage devices” as required.

B. Petitioner’s Dickinson-Takeda Ground Fails (All Claims, Ground 4).

1. The ’140 And Dickinson

100. I have been informed and understand that Dickinson is Patent Owner’s patent application with three out of four named inventors in common. I also understand that Dickinson was disclosed to the Examiner in an IDS and was explicitly considered by the Examiner. Ex. 1002 [Pros-Hist] 165-166, 299, 1234-1242, 1360-1361. While Dickinson’s Figures 1-20 and its specification are largely

included in the '140's specification, the '140 includes ***40 new figures and over forty-five columns of new material*** not present in Dickinson. Compare Ex. 1005 [Dickinson] with Ex. 1001 ['140] Figs. 21-60, 1:1-2:26, 2:30-58, 3:44-6:45, 7:41-9:12, 10:40-41, 10:63-65, 18:56, 19:12-15, 20:20-22, 20:38-39, 20:48-50, 21:1-3, 21:24-40, 22:13-21, 30:53-55, 34:7-12, 36:60-64, 37:36-40, 44:42-44, 52:55-99:23.

101. Dickinson is further directed to an earlier and different invention of the inventors, namely, a “trust engine” for “facilitating an authentication relating to an electronic transaction between a first and a second user.” Ex. 1005 [Dickinson] Abstract. This is distinct from the '140.

102. Dickinson is directed to a “trust engine” for “accessing and storing sensitive information, such as user authentication data and public and private encryption keys” that can be used to “uniquely identify a user” of the system. Ex. 1005 [Dickinson] 10:20-23. Examples of data accessible using the trust engine include “a user identification number, one or more biometrics, [or] a series of questions and answers ... answered initially by the user at enrollment.” *Id.*, 10:23-25. The trust engine compares the authentication data provided by the user in “a current transaction[] to the authentication data provided at an earlier time, such as ... during enrollment.” *Id.*, 10:27-29. “Once the user produces the appropriate [current] authentication data and the trust engine 110 determines a positive match” with the stored data “provided at the time of enrollment (enrollment authentication

data), the trust engine 110 provides” functionality to securely complete the current transaction, such as “hashing, digitally signing, encrypting and decrypting, ... distributing digital certificates, and the like.” *Id.*, 11:3-9.

103. Notably, in contrast to the claimed inventions, Dickinson’s trust engine does not present a virtual disk of any sort to the user. In fact, the opposite is true: the user provides authentication data to the trust engine, data that can be compared to the authentication data already securely stored within the trust engine. For example, a user may provide a fingerprint to verify his or her identity to facilitate the issuance of a digital certificate by a certificate authority. The trust engine receives digitized fingerprint data from reader and compares it to fingerprint data for that user previously stored within the trust engine during enrollment. If it finds a match, the trust engine may transmit a request to the certificate authority. Dickinson’s trust engine is shown in relation to the user and the certificate authority in Figure 1:

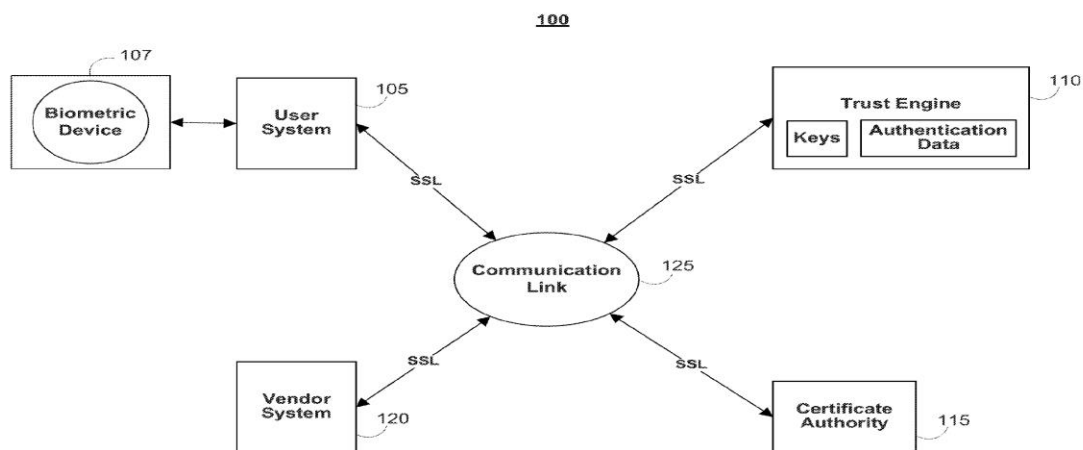


FIG. 1

Id., Fig. 1.

104. Dickinson's trust engine is comprised of several modules, as shown in its Figure 2, including a transaction engine for communicating through a communications link with users and third parties. The modules also comprise (1) a depository for storing enrollment authentication data and cryptographic key data, (2) an authentication engine for comparing enrollment authentication data provided by the depository to current authentication data, and (3) a cryptographic engine to provide required cryptographic services if the user is authenticated. *See generally id.*, 13:5-15:33. Notably, as shown in Figure 2, the transaction engine is the only module that communicates with users outside the trust engine.

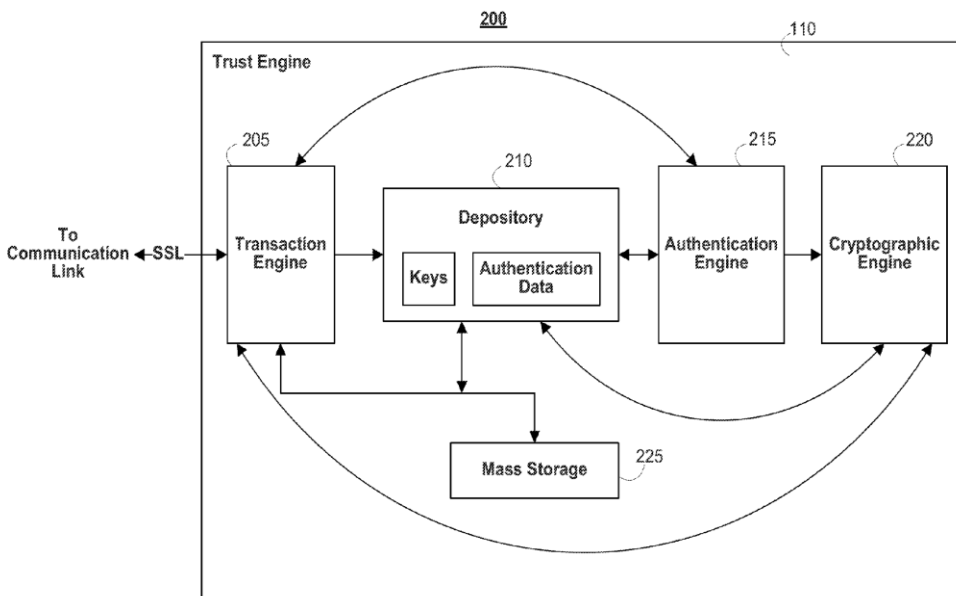


FIG. 2

Id., Fig. 2.

105. The depository 210 “comprises one or more lightweight directory access protocol (LDAP) servers” used to store enrollment authentication data. *Id.*, 16:25-29. Depository 210, shown in Figure 4 below, may then comprise “a single logical memory structure indexing authentication data ... to a unique user ID.” *Id.*, 16:28-31, 17:4-5.¹ As shown on the right side of Figure 4, the depository provides

¹ Petitioner misleadingly suggests that Dickinson equates its “single logical memory structure indexing authentication data ... to a unique user ID” to a “virtual disk.” Pet., 71-72. However, there is no such disclosure in Dickinson—in fact, the term “virtual” is not used in the reference.

data to the trust engine's mass storage, to the authentication engine, and to its cryptographic engine, but does not provide data outside the trust engine.

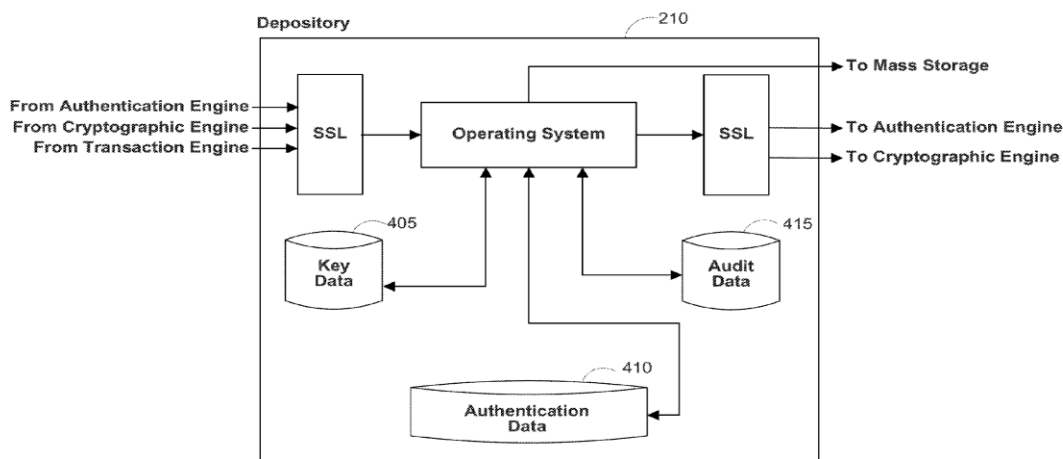


FIG. 4

Id., Fig. 4.

106. As shown in Figure 7 below, Dickinson's depository may comprise "distinct and physically separated data storage facilities," shown as D1-D4. *Id.*, 17:4-5. Each data storage facility "may ... comprise some or all of the elements disclosed with reference to depository 210 of Figure 4." *Id.*, 19:19-20.

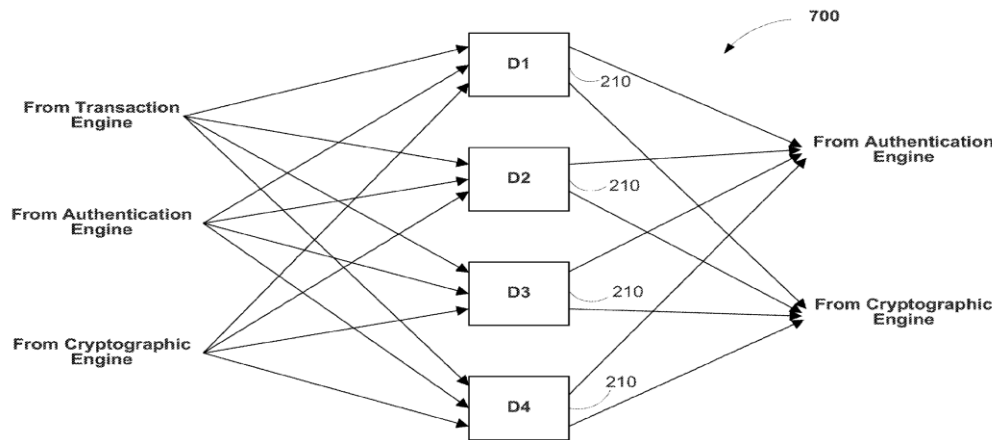


FIG. 7

Id., Fig. 7.

107. In one embodiment, the authentication engine includes a “splitting module” to divide enrollment authentication data into one or more “portions” or shares, and different shares of that data may be stored in different storage facilities to promote data security, availability and redundancy. *Id.*, 19:31-34, 20:1-14.

108. Dickinson’s disclosures above show that the only common feature between Dickinson and the ’140 is that both inventions may store a plurality of shares across a plurality of storage devices. There is, however, no disclosure that Dickinson’s depository presents a virtual disk to a client system. Specifically, there is no disclosure in Dickinson that any information about the “logical memory structure,” Petitioner’s purported “virtual disk,” is presented to the trust engine’s users. Nor is there any disclosure regarding what that “logical memory structure” in depository 210 comprises, beyond authentication and cryptographic data, or

what it may be mapped to. These are features explicitly discussed in the '140 specification that are missing in Dickinson's specification.

109. As I discussed above, the '140 added new content over Dickinson in the amount of 40 new figures and over forty-five columns of new material. Much of this new content directly relates to claim 1's "virtual disk" limitation.

110. Limitation 1[b][1], again, requires "a secure storage system configured to" "present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device." Limitation 1[b][1] is disclosed in the '140, but not in Dickinson.

111. The '140, but not Dickinson, introduces a "Parsed File System (PFS)" which, as will be shown, is an example of limitation 1[b][1]:

A Parsed File System (PFS) *is a distributed file system which incorporates a directory*, shared among file servers, which is itself parsed. *The PFS directory is the clients' view of all file assets*. The set of files visible to an individual client is controlled by that client's group keys. *The PFS may maintain a directory that contains information about the locations of the shares (for example, the file server location) and the names of the files at the share locations that include the share data.*

...

The underlying distribution of shares may be hidden from users/clients by the PFS such that files appear as a file storage system based on the PFS directory. The PFS provides an interface that allows users to access parsed files without knowledge of the location of shares.

Id., 87:16-43.

112. Thus, in accordance with limitation 1[b][1], the PFS is, *e.g.*, “a distributed file system which incorporates a directory.” *Id.*, 87:16-18. The “PFS directory is the clients’ view of all file assets” and, thus, is “present[ed] to a client device.” *Id.*, 87:18-19. The PFS directory is “mapped to the plurality of physical storage devices,” as it may “contain[] information about the locations of the shares (for example, the file server location) and the names of the files at the share locations that include the share data.” *Id.*, 87:20-24. The PFS directory, moreover, “provides an interface that allows users to access parsed files ***without knowledge of the locations of shares***,” showing the directory may be mapped “such that physical locations of the shares are hidden from the client device.” *Id.*, 87:37-39.

113. The ’140, thus, teaches a “virtual disk” (*e.g.*, the PFS which is a distributed file system²), “present[ed] to a client device” (the PFS directory is “the

² The PFS as described at Ex. 1001 [’140] 87:16-43 is an example of a “virtual disk” under both parties proffered claim constructions. Petitioner contends

clients' view of all file assets") which comprises a "directory" (e.g., the PFS "directory"), "mapped to the plurality of physical storage devices" (the PFS directory may contain "information about the location of the shares" and "the names of the files at the share locations that include the share data"), "such that physical locations of the shares are hidden from the client device" (the PFS directory provides "an interface allowing the users to access parsed files without knowledge of the locations of shares").

114. The PFS directory is disclosed in the '140 but not in Dickinson. *Compare* Ex. 1001 ['140] 87:16-88:56 with *generally* Ex. 1005 [Dickinson]. Petitioner and Dr. Bhattacharjee further ignore the '140's teachings relating to the PFS directory. And, as discussed below, Petitioner does not demonstrate that Dickinson discloses a "directory," much less one that is a "clients' view of all file assets." Nor is there any indication in Dickinson that there is an "interface that

a "virtual disk" is "a distributed file system shared among file servers." Ex. 1041 [Pet-CC] 10. The PFS clearly satisfies this construction as it is explicitly named as "a distributed file system...shared among file servers." Ex. 1001 ['140] 87:16-18. Patent Owner contends a "virtual disk" requires "no construction," but in the alternative contends it is "a system that simulates or emulates a physical storage device." Ex. 1042 [PO-CC] 10.

allows users to access parsed files without knowledge of the location of shares.”

Ex. 1001 [’140] 87:37-39. Thus, Dickinson simply fails to show any of these new teachings in the ’140.

115. Additionally, limitation 1[b][3] of claim 1 requires “includ[ing] with each of the plurality of shares data indicative of the at least one session key used to secure the dataset” (1[b][3]). Dickinson, in my opinion, lacks the disclosure for this limitation, which is included in the ’140’s new material.

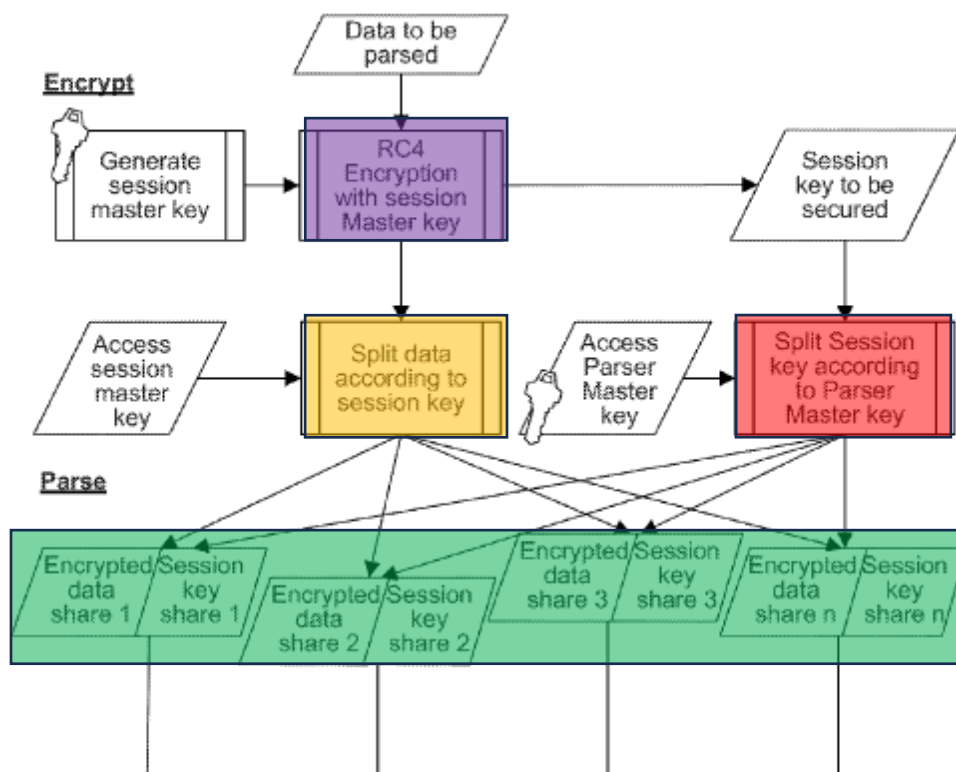
116. Dickinson introduces and discusses a “session key,” but only in connection with Figure 12. *See, e.g.*, Ex. 1005 [Dickinson] 32:26-31; Fig. 12. But nowhere in Dickinson’s discussion of Figure 12 is a “plurality of shares” even mentioned (1[a]) much less “includ[ing] with the plurality of shares data indicative of the at least one session key” as required by limitation 1[b][3]. *See* Ex. 1005 [Dickinson] 32:26-31.

117. In any event, Petitioner does not even rely on Dickinson’s teachings relating to a “session key” to satisfy limitation 1[b][3], or limitation 1[a] (also concerning a “session key”) for that matter. Petitioner instead relies upon Dickinson’s teachings relating to Figure 8, which do not mention or concern session keys at all. *See* Pet., 69-70.

118. Indeed, substantial additions to the ’140 over Dickinson focus upon the handling of “session keys.” Indeed, session keys are mentioned 108 times in

the '140 patent, and 93 of these instances are only in the '140. Session keys are, moreover, a feature in eight new figures (Figs. 21-24, 33-35, 39) and are further discussed in connection with eight more figures. *Id.*, 71:12-21 (Fig. 30), 76:4-49 (Fig. 36), 76:62-77:4 (Fig. 37), 77:5-33 (Fig. 38), 78:20-40 (Fig. 40), 83:31-50 (Fig. 46), 85:33-53 (Fig. 46), 87:3-15 (Fig. 47). Thus, there is an enormous expansion on the teaching of a “session key” in the '140, as compared to Dickinson.

119. As just one example, new Figure 21 teaches encrypting a dataset with a “session master key,” separating the encrypted data into four shares according to the pattern of the session master key, separating the session master key according to the parser master key and appending the key data to the encrypted parsed data, wherein “[t]he resulting four shares of data will contain encrypted portions of the original data and portions of the session master key.” Ex. 1001 ['140] 56:19-36.



Ex. 1001 ['140] Fig. 21 (annotated).

120. Thus, among other new, relevant disclosures in the '140, Figure 21 in the '140 teaches “a plurality of shares” “associated with at least one session key” (1[a]) and storing “data indicative of the at least one session key with each of the plurality of shares” (1[b][3]). There is no corresponding teaching in Dickinson.

2. Dickinson And Petitioner’s Arguments Were Expressly Considered By The Examiner In Prosecution

121. I understand that Dickinson was disclosed by the Applicant during patent prosecution, and was considered and rejected by the Examiner with respect to two limitations.

122. Limitation 1[b][1] requires a “secure storage system configured to” “present to a client device a virtual disk ... comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device.”

123. It is my understanding that Petitioner contends Dickinson discloses or renders obvious the “virtual disk” limitation 1[b][1]. Pet., 71-74. It is also my understanding that the Examiner considered this argument and had determined that “Dickinson...**does not explicitly disclose the limitation** such that the virtual disk comprising the directory mapping to the plurality of storage device [sic].” Ex. 1002 [Pros-Hist] 1239. I note the Examiner cited the very portion of Dickinson Petitioner now contends discloses the “virtual disk” limitation. Ex. 1002 [Pros.-Hist.] 1237-1238 (citing Ex. 1005 [Dickinson] 16:28-31). I see no error in the Examiner’s conclusion.

124. Limitation 1[b][3] requires includ[ing] with each of the plurality of shares data indicative of the at least one session key used to secure the dataset.” I note this limitation was specifically added during prosecution to overcome Dickinson, where the Applicant stated:

Independent claim 14 has been amended to recite, *inter alia*, a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset, and a secure storage system

configured to generate the plurality of shares and ***include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset.*** Independent claim 14 patentably improves upon the combination of Dickinson and Bendix because neither Dickinson nor Bendix teach or suggest storing any additional information with each of the data shares, much less information used to secure a dataset. For example, Dickinson describes a data splitting process 800 in which *transformed versions* of an *entire* set of data "S" are stored in multiple data storage facilities. *See, for example*, pp. 21-22 and FIG. 8 at step 805. However, Dickinson does not teach or suggest ***including with each of the plurality of shares data indicative of the at least one session key used to secure the dataset***, as claimed. Bendix also fails to teach or suggest this subject matter, and nowhere does the Examiner contend that it might.

Ex. 1002 [Pros.-Hist.] 1245-1246 (emphasis in original). The Examiner confirmed that "Applicant's arguments ... have been fully considered and are persuasive," and correctly allowed the claims. Ex. 1002 [Pros-Hist] 1360.

125. Dickinson, on which Petitioner relies, is the same art as that addressed by the Examiner in prosecution. I also note that Petitioner asserts the same arguments which were already considered and rejected by the Examiner. I see no error on the Examiner's part in concluding that Dickinson does not disclose storing data indicative of a session key with each of the shares.

3. “A Secure Storage System Configured To:” “Present To A Client Device A Virtual Disk, The Virtual Disk Comprising A Directory Mapped To The Plurality Of Physical Storage Devices Such That Physical Locations Of The Shares Are Hidden From The Client Device” (Limitation 1[b][1]).

126. Claim 1 requires:

Limitation 1[b][1] “secure storage system configured to:” “present to a client device a virtual disk ... comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device.”

- a. *Dickinson Does Not Disclose Or Render Obvious “A Directory.”*

127. I do not believe Petitioner or Dr. Bhattacharjee have demonstrated that Dickinson’s purported index is a “directory” as required.

- b. *Dickinson Does Not Disclose Or Render Obvious A Directory “Mapped To The Plurality Of Physical Storage Devices.”*

128. Even if, for the sake of argument, Dickinson’s indexing results in an index, and even if the index is considered a directory, Petitioner and Dr. Bhattacharjee fail to demonstrate that any such directory would be “mapped to the plurality of physical storage devices.”

129. Petitioner asserts that Dickinson discloses a “directory” in depository 210 which is “mapped to the plurality of physical storage devices,” D1-D4. To support this proposition, Petitioner points to Dickinson’s statement that “the depository 210 comprises a single logical memory structure...” (Ex. 1005, 16:29-

31) and an additional teaching that “the depository 210 may comprise distinct and physically separated data storage facilities, as disclosed further with reference to Figure 7” (*id.*, 17:4-5). Pet., 71 (“Dickinson’s depository 210, which may comprise FIG. 7’s storage facilities D1-D4, comprises a single logical memory structure.”). Thus, Petitioner seems to suggest that because depository 210 includes a single logical memory structure and may further include D1-D4 in the Figure 7 embodiment, the alleged index in depository 210 would be “mapped” to D1-D4.

130. But Dickinson’s discussion of Figure 7 does not suggest that each of D1-D4 is a part of a single depository 210. Rather, Figure 7 identifies *each* of the depositories in depository system 700 as its own depository 210.

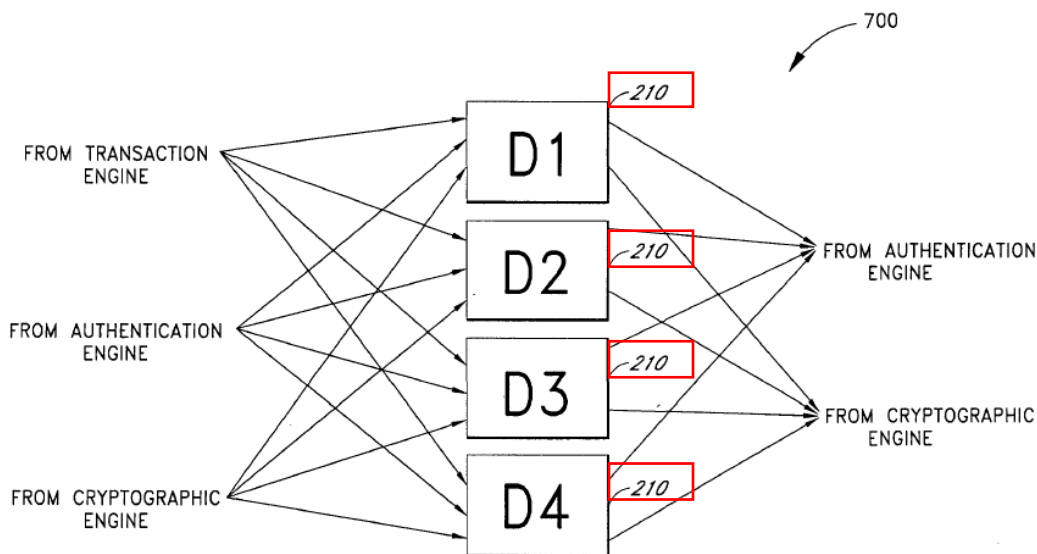


FIG. 7

Ex. 1005 [Dickinson] Fig. 7 (annotated). In the same vein, Dickinson teaches that “each of the data storage facilities D1 through D4 may advantageously comprise some or all of the elements disclosed with reference to the depository 210 of FIGURE 4.” *Id.*, 19:17-20. Dickinson further teaches that “each data storage facility, D1 through D4, comprises a separate and **independent** storage system” including in the depository system 700 embodiment. *Id.*, 20:1-3.

131. Consequently, each of D1-D4 is separate and independent, and would include its own depository 210 with its own “logical memory structure indexing authentication data and cryptographic key data to a unique user ID.” *Id.*, 16:30-31. Thus, there would be no need for an index or directory mapped to each of D1-D4. In accord, while each data storage facility may receive requests from various engines (the transaction engine, the authentication engine, and the cryptographic engine), there is no teaching that any given storage facility may make requests to other storage facilities or that each instantiation of depository 210 holds a “directory” mapped to the other storage facilities. *Id.*, 19:17-24.

132. I understand that Petitioner and Dr. Bhattacharjee “alternatively” contend that Dickinson renders claim 1 obvious:

To the extent Dickinson is read to not expressly disclose a directory with this mapping, that would have been the conventional and obvious way to implement Dickinson’s logical memory structure so that each piece of sensitive data S included in that logical memory structure can

be retrieved from data storage facilities D1-D4 when desired.
Bhattacharjee, ¶231.

Pet., 73. In my opinion, they have failed to demonstrate so.

133. Petitioner contends that it would be conventional and obvious to “implement Dickinson’s logical memory structure so that each piece of sensitive data S included in that logical memory structure can be retrieved from data storage facilities D1-D4 when desired.” Pet., 73. But this contention does not follow, and it is contrary to Dickinson’s disclosure. Petitioner seems to imagine a logical memory structure interacting with and retrieving data from various data storage facilities D1-D4. But Dickinson, instead, teaches that each of storage facilities D1-D4 is a separate and independent instantiation of depository 210, each with its own logical memory structure. *See* Ex. 1005 [Dickinson] 19:16-20; 16:29-31; Fig. 7. Each of D1-D4 may receive requests directly from various engines. *Id.*, 19:20-26. The embodiments Petitioner relies upon in its discussion regarding limitation 1[a] requiring a “plurality of physical storage devices” also twice states that the facilities are “separate” and “independent.” *Id.*, 20:1-3; Pet., 68. Because each of D1-D4 operates independently, includes its own logical memory structure, and receives requests independently, there is no need for a “directory” mapped to D1-D4.

134. In this regard, Dickinson's disclosure is unlike the '140's discussion of the "PFS directory" which "may maintain a directory that contains information about the location of the shares (for example, the file server location) and the names of the files at the share locations that include the share data." Ex. 1001 ['140] 87:20-23.

135. Thus, I do not believe Petitioner or Dr. Bhattacharjee have demonstrated that Dickinson discloses or renders obvious a "directory mapped to the plurality of physical storage devices."

c. Dickinson Does Not Disclose Or Render Obvious "That Physical Locations Of The Shares Are Hidden From the Client Device."

136. Petitioner further fails to demonstrate that Dickinson discloses that the "physical locations of the shares are hidden from the client device," as limitation 1[b][1] requires.

137. Petitioner and Dr. Bhattacharjee assert that "the actual physical data storage facilities (*e.g.*, D1-D4) on which the data is stored are hidden from the user":

That logical memory structure is a virtual disk under SFI's construction because it is a virtual ('logical') representation of storage that appears to the user to be a physical disk but where the actual physical data storage facilities (*e.g.*, D1-D4) on which the data is stored are hidden from the user. Ex. 1005 [Dickinson] 16:28-31, 29:12-30:2; Ex. 1003 [Bhattacharjee] ¶229.

Pet., 71-72. In my opinion, Petitioner and Dr. Bhattacharjee fail to substantiate their assertion.

138. Petitioner and Dr. Bhattacharjee's cited evidence does not support the conclusion that the physical locations of the shares are hidden from the client device. Petitioner cites Dickinson at 16:28-31 and 29:12-30:2 but those passages have nothing to do with hiding the physical locations of the shares from the client device. *See* Ex. 1005 [Dickinson] 16:28-31, 29:12-30:2. Dickinson at 16:28-31 does not mention hiding the location of shares from the client device or storage facilities D1-D4. *Id.*, 16:28-31 ("FIGURE 4 also shows that the directory server preferably stores data 405 corresponding to the cryptographic keys and data 410 corresponding to the enrollment authentication data. According to one embodiment, the depository 210 comprises a single logical memory structure indexing authentication data and cryptographic key data to a unique user ID."). Dickinson at 29:12-30:2 is equally irrelevant. It concerns a "sensitive data vault" in the context of "authentication process 1000" and its various embodiments:

In addition, the authentication process 1000 may [] advantageously be employed to develop elegant single sign-on solutions, such as, unlocking a sensitive data vault. For example, successful or positive authentication may provide the authenticated user the ability to automatically access any number of passwords for an almost limitless number of systems and applications. For example, authentication of a user may provide the user access to password,

login, financial credentials, or the like, associated with multiple online vendors, a local area network, various personal computing devices, Internet service providers, auction providers, investment brokerages, or the like. By employing a sensitive data vault, users may choose truly large and random passwords because they no longer need to remember them through association. Rather, the authentication process 1000 provides access thereto. For example, a user may choose a random alphanumeric string that is twenty plus digits in length rather than something associated with a memorable data, name, etc.

According to one embodiment, a sensitive data vault associated with a given user may advantageously be stored in the data storage facilities of the depository 210, or split and stored in the depository system 700. According to this embodiment, after positive user authentication, the trust engine 110 serves the requested sensitive data, such as, for example, to the appropriate password to the requesting application. According to another embodiment, the trust engine 110 may include a separate system for storing the sensitive data vault. For example, the trust engine 110 may include a stand-alone software engine implementing the data vault functionality and figuratively residing “behind” the foregoing front-end security system of the trust engine 110. According to this embodiment, the software engine serves the requested sensitive data after the software engine receives a signal indicating positive user authentication from the trust engine 110.

In yet another embodiment, the data vault may be implemented by a third-party system. Similar to the software engine embodiment, the third-party system may advantageously serve the requested sensitive data after the third-party system receives a signal indicating positive user authentication from the trust engine 110. According to yet another embodiment, the data vault may be implemented on the user system 105. A user-side software engine may advantageously serve the foregoing data after receiving a signal indicating positive user authentication from the trust engine 110.

Id., 29:12-30:2. The only mention of data storage facilities D1-D4 in this Dickinson excerpt is that the sensitive data vault may be “split and stored in the depository system 700.” *Id.* There is no suggestion therein that the physical locations of the shares are “hidden from the client device.”

139. Dickinson’s lack of disclosure, moreover, lies in stark contrast with the ’140’s clarity, which provides that “[t]he underlying distribution of shares **may be hidden from users/clients**” and “[t]he PFS provides an interface that allows users to access parsed files **without knowledge of the location of shares.**” Ex. 1001 [’140] 87:35-39.

140. Thus, I do not believe Petitioner or Dr. Bhattacharjee have demonstrated that Dickinson discloses or renders obvious presenting to the client device a directory “such that physical locations of the shares are hidden from the client device.”

d. *Dickinson Does Not Disclose Or Render Obvious “A Secure Storage System Configured To: “Present To A Client Device A Virtual Disk.”*

141. To reiterate, the claims require “a secure storage system configured to: present to a client device a virtual disk” (limitation 1[b][1]). Petitioner identifies Dickinson’s data vault and transaction engines as comprising the “secure storage system.” Pet., 70, 71. Petitioner relies on the “logical memory structure” of depository 210 as a “virtual disk” in an attempt to show Dickinson meets this limitation.

142. Petitioner contends the “logical memory structure” is presented to the client device by the “transaction engine” “[w]hen the user system 105 requests the sensitive data from the sensitive data vault.” Pet., 73. Petitioner, however, does not prove this.

143. There is, quite simply, no reason to believe that the **logical memory structure** is presented to the user when the user requests sensitive data. When user system 105 requests data from the sensitive data vault of the “data vault engine,” Dickinson teaches that an authentication process commences. Ex. 1005 [Dickinson] 29:17-19. Therein, the “authentication engine” compares the user’s login information with its enrollment information in depository 210. *Id.*, 15:4-12. If the user is authenticated, **sensitive data from the sensitive data vault is served to the user.** *Id.*, 29:25-30.

144. Thus, when the user requests sensitive data, upon verification, “sensitive data ... is served to the user.” There is no indication, however, that **the “logical memory structure”** (Petitioner’s alleged “virtual disk”) is presented to the user. The sensitive data and the logical memory structure are two different things. The logical memory structure stores “[enrollment] authentication data and cryptographic key data [for] a unique user ID.” Ex. 1005 [Dickinson] 16:28-31; *id.*, 14:17-19. Its role is to facilitate the authentication of users seeking to access sensitive data. It, itself, is highly sensitive as it contains login/authentication information for a specific user. Dickinson does not disclose “presenting” the logical memory structure to the user and it’s not self-evident why it would.

145. Petitioner and Dr. Bhattacharjee further contend that it is the transaction engine 205, of the trust engine 110, that “presents” the logical memory device to the client. See Pet., 73 (“When the user system 105 requests the sensitive data from the sensitive data vault, the logical memory structure (‘virtual disk’) is presented to the [client device] **by the transaction engine...**”). I disagree.

146. Contrary to Petitioner’s contention (Pet., 73), Dickinson does not disclose that the transaction engine “presents” the “logical memory structure” (in depository 210) to the client device. Dickinson discloses that the transaction engine “comprises a data routing device,” that may route data **to** “one of the depository 210, the authentication engine 215, the cryptographic engine 220, and

the mass storage 225.” Ex. 1005 [Dickinson] 13:18-19, 13:23-25. The transaction engine also routes data from the authentication and cryptographic engines to the user system 105. *Id.*, 13:25-28.

147. Dickinson, however, makes no mention of routing the logical memory structure, or anything else, **from depository 210** to the client device. As Figure 2 further illustrates, the transaction engine 205 may route requests to depository 210, **but**, there is no indication the transaction engine presents depository 210 or its logical memory structure to the client device:

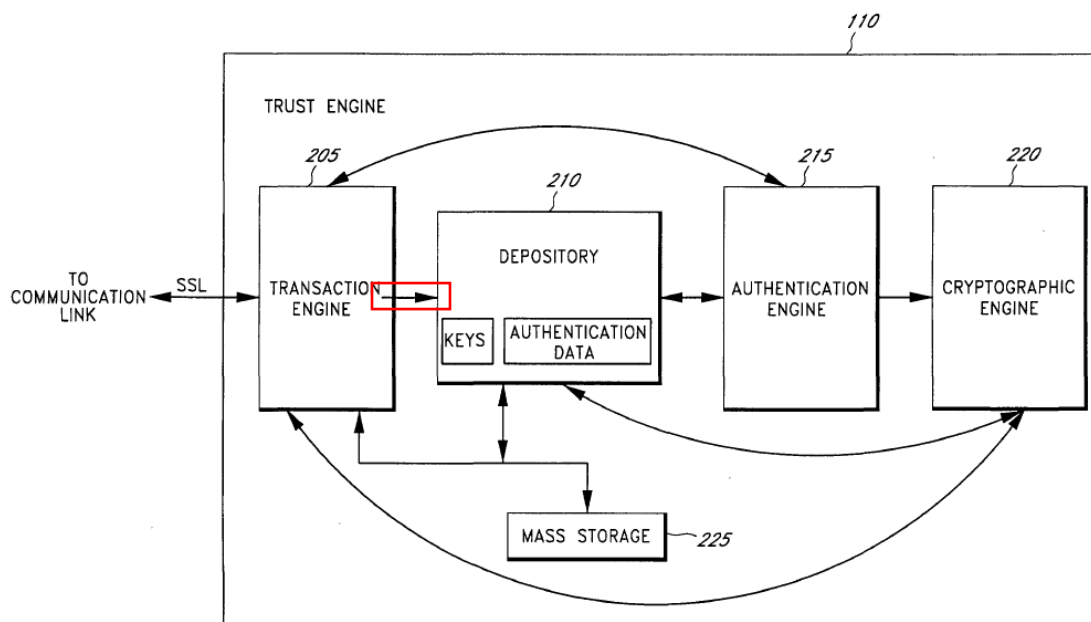


FIG. 2

Ex. 1005 [Dickinson] Fig. 2 (annotated). The one-way arrow between the transaction engine and depository 210 indicates that the transaction engine may transmit data to depository 210 but nothing identified in this figure or Dickinson’s

disclosure suggests the logical memory structure or anything else in depository 210 is presented by the transaction engine to the client device/user.

148. In accord, Figure 4 further confirms that depository 210 receives data from the transaction engine but does not send data to the transaction engine:

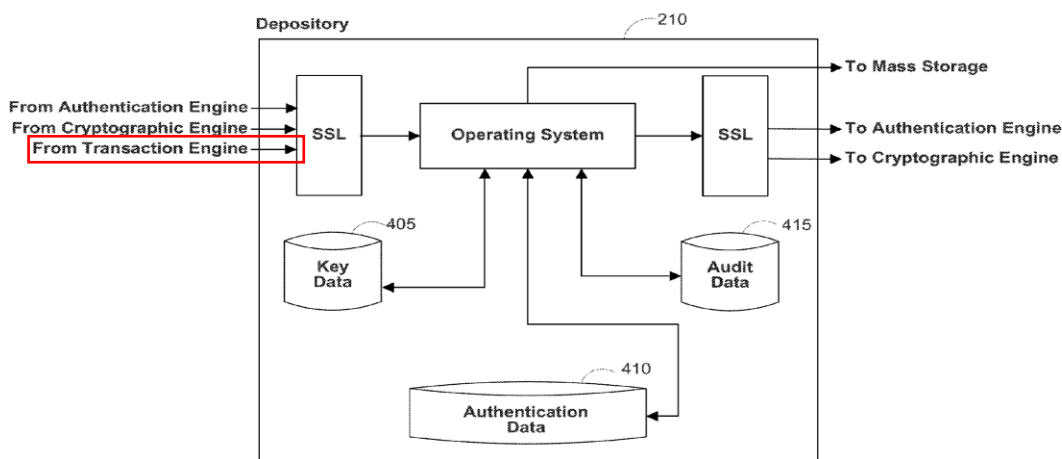


FIG. 4

Ex. 1001 [’140] Fig. 4.

149. Nor would the “logical memory structure” of depository 210 be routed through the authentication engine 215 or cryptographic engine 220 to the transaction engine 205 and the user system 105. While Dickinson discloses that the “transaction engine 205 monitors incoming *data* from the authentication engine 215 and cryptographic engine 220” and “may advantageously route data to the user system 105,” there is no disclosure that the “logical memory structure,” as the purported virtual disk, would be presented to the “user system 105.” Ex. 1005

[Dickinson] 13:25-28. Dickinson instead explicitly discloses that “the trust engine,” which houses the respective engines discussed above, “does **not** release actual keys and other authentication data, and therefore, the keys and data remain secure.” *Id.*, 9:9-11. The keys and other authentication data are precisely the types of data stored within the “logical memory structure” (*id.*, 16:28-31), and Dickinson makes quite clear that it is not released to the client.

150. Thus, in my opinion, a POSITA would not be motivated to present any information within the depository 210 to the client device.

151. Petitioner further contends that “a POSA would have understood that in the embodiment that has a data vault engine, the data stored therein is included in the index of the user’s data.” *Pet.*, 72. This contention appears to be ultimately irrelevant, as even if the data stored in the data vault engine was included in the purported “index,” it does not show the presentation of the logical memory structure to the client device by a “secure storage system.”

152. Petitioner alternatively contends that even if Dickinson does not “expressly disclose that the logical memory structure is presented to the user system 105, that would have been an obvious way to implement what Dickinson describes ...” *Pet.*, 72-74. Petitioner’s contention, however, appears to be ultimately irrelevant, because the claims require a “**secure storage system** configured to” “present to a client device a virtual disk.” Thus, even if a POSITA

were motivated to present the logical memory structure to the client device, there is no teaching that this would occur vis-à-vis the transaction engine and/or the data vault engine, which are the only components Petitioner contends comprise the secure storage system.

153. There is further no indication a POSITA would be motivated to present the logical memory structure to the client device.

154. Under Dickinson's current structure, as described above, an authentication engine compares a login attempt with enrollment data to determine whether a user login attempt is successful. Ex. 1005 [Dickinson] 17:6-35. There is no reason to alter Dickinson such that the user device would have direct access to the logical memory structure which contains both "authentication data and cryptographic key data." *Id.*, 16:28-31. This would result in a system that is less secure and for no discernible benefit.

155. Petitioner further argues that including "the data stored" in the data vault engine "in the index of the user's data ... would have been the obvious way to implement what Dickinson describes so that the user can see all the user's stored data in the index and retrieve the data the user desires to access." Pet., 72. This argument appears similarly irrelevant, as Petitioner still fails to show it would be obvious for the "secure storage system" (*e.g.*, the transaction engine) to present a

logical memory structure “indexing authentication data and cryptographic key data to a unique user ID” (Ex. 1005, 16:28-31) to the client device.

156. Consequently, I do not believe Petitioner or Dr. Bhattacharjee have demonstrated that Dickinson discloses or renders obvious the limitation requiring “a secure storage system configured to:” “present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device.”

4. “Plurality Of Shares” “Associated With At Least One Session Key Used To Secure A Dataset” (Limitation 1[a]) “Include With Each Of The Plurality Of Shares Data Indicative Of The At Least One Session Key” (Limitation 1[b][3]).

157. Claim 1 requires:

Limitation 1[a] “a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset; and”

Limitation 1[b][3] “include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset.”

158. Petitioner and Dr. Bhattacharjee contend that Dickinson, alone and without modification, discloses limitation 1[b][3]. Pet., 60, 64, 74; Ex. 1003 [Bhattacharjee] ¶¶ 203, 216, 238. Petitioner and Dr. Bhattacharjee rely on Dickinson’s Figure 8 for this assertion. Pet., 64-65; Ex. 1003 [Bhattacharjee] ¶ 216. But all of Dickinson’s discussion of “session keys” arises in relation with

Figure 12, which Petitioner does not rely upon. Thus, in my opinion, Figure 8 teaches no such thing.

159. Even if, assuming for the sake of argument, “A” and “C” are session keys, Dickinson does not disclose including data indicative of the session keys with shares “B” and “D,” as limitation 1[b][3] requires.

160. The Applicant in prosecution pointed out that Dickinson describes a data splitting process 800 in which *transformed versions* of an *entire* set of data ‘S,’ not data indicative of session keys used to secure the dataset, are stored in multiple data storage facilities. *See* Ex. 1002 [Pros.-Hist.] 1245-6 (citing Ex. 1005 [Dickinson] 21-22, Fig. 8). Based on Dickinson’s described process, this is accurate. Dickinson discloses in Figure 8 that dataset “S” is received and a data splitting module generates random numbers “A” and “C.” Ex. 1005 [Dickinson] 20:23-32. “S” is “transformed” because it is combined in whole with the number “A” and again with the number “C” resulting in the new numbers “B” and “D.” Dickinson explains that the “number B may comprise the binary combination of A XOR S and [the] number D may comprise the binary combination of C XOR S.” Ex. 1005 [Dickinson] 20:33-34. No data from the purported “session keys,” “A” and “C,” are included within the purported shares, “B” and “D.” Instead, “A” and “C” are separate files that must be separately stored and recovered to reassemble dataset “S.” *See id.*, 21:1-14.

161. Thus, both “B” and “D” are each “transformed” versions of the entire dataset “S”; they do not teach or suggest storing **any additional information** with each of the data shares, much less information used to secure a dataset (*i.e.*, “data indicative of a session key”).

162. Thus, in my opinion, Dickinson alone does not disclose limitation 1[b][3]’s requirement of “includ[ing] with each of the plurality of shares data indicative of the at least one session key used to secure the dataset.”

163. Petitioner and Dr. Bhattacharjee alternatively contend a combination of Dickinson and Takeda meets limitation 1[b][3]. These contentions fail because a POSITA would also not be motivated to modify Dickinson in view of Takeda, as each of Petitioner’s proffered motivations offers no benefit and entails distinct drawbacks to Dickinson’s system.

164. Petitioner and Dr. Bhattacharjee contend that a POSITA would be motivated to modify Dickinson’s storage of data shares and session keys in “depository system 700” such that “a pointer to and/or metadata of” a session key is stored with a data share instead of a session key itself. Pet., 61. Petitioner bases this argument on the contention that Dickinson “does not specify how its system knows where to retrieve the correct key ... for decrypting the corresponding encrypted data portion ... to recover S.” Pet., 61 (citing Ex. 1003 [Bhattacharjee] ¶204). However, Dickinson is intentionally designed such that “only data from

two of the multiple data storage facilities, D1 through D4, are needed to decipher and reassemble the sensitive data,” dataset “S.” Ex. 1005 [Dickinson] 20:4-7. This configuration “provides redundancy along with additional security measures,” while also allowing the “data stored in each data storage facility [to be] randomized and undecipherable, [so that] compromise of any individual data storage facility does not necessarily compromise the sensitive data.” *Id.*, 20:4-7, 20:9-11. This design obviates the need for Dickinson’s system to “know” where to retrieve the session keys, as redundancy and randomization are intentionally contemplated.

165. Petitioner and Dr. Bhattacharjee further contend a POSITA would be motivated to modify Dickinson with Takeda to “beneficially allow[] for separate management of the encrypted data and the keys for that data, for example to best use limited storage space.” Pet., 61. But the storage of a pointer to and/or metadata of a key, rather than the key itself, would come at the cost of the specifically contemplated benefit of redundancy addressed earlier. Neither Petitioner nor Dr. Bhattacharjee suggest *where* the actual keys would be stored in the proposed combination, aside from a citation to a different reference, Ophir, indicating it may be placed in some “external storage.” Pet., 61 (citing Ex. 1007 [Ophir] ¶32). But this storage scheme would result in the loss of Dickinson’s ability to reassemble the dataset by only recovering data from two of the four data

storage facilities. It may even further complicate Dickinson’s recovery process, as Dickinson would need to access an undisclosed storage facility outside of its current storage scheme, which may be less secure than its depositories, to recover random numbers “A” and “C.” This drawback would dissuade a POSITA from modifying Dickinson as Petitioner and its expert contemplate.

166. Petitioner and its expert also assert that a POSITA would be motivated to combine references because the metadata could be used “beneficially during decryption.” Pet., 61. But this is no motivation, as Dickinson’s random numbers “A” and “C” themselves, as the supposed “keys,” would be at least as beneficial to decrypt the “shares” as mere metadata. Petitioner and Dr. Bhattacharjee fail to explain exactly **why** the metadata for a key would be preferable to the key itself in terms of decryption. *See id.*; Ex. 1003 [Bhattacharjee] ¶207.

167. Petitioner and its expert also fail to disclose any benefit associated with the provision of “a technique for providing the association between the encrypted data portion and its key” such that “the correspondence relation between the data can be recognized” would render. Pet., 61. Petitioner simply asserts, without explanation, that the combination “would have motivated POSAs to use that technique to provide that association in Dickinson.” Pet., 62 (citing to Ex. 1003 [Bhattacharjee] ¶209). Petitioner’s expert also opines at ¶209, without

explanation, that “a POSA...would need a way to associate data with corresponding keys in order to reconstruct the original data.” But, as discussed above, Dickinson as configured can already reconstruct the original data by recovering from only two of four storage facilities. Ex. 1005 [Dickinson] 20:6-7.

168. Thus, I do not believe Petitioner or Dr. Bhattacharjee have demonstrated that Dickinson, or Dickinson and Takeda in combination, disclose or render obvious the requirement to “include with the plurality of shares data indicative of the at least one session key used to secure the dataset.”

169. 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.

VII. CONCLUSION

170. 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 1-10 are not disclosed by or obvious over Ophir and Takeda;
- Claims 1-10 are not disclosed by or obvious over Dickinson and Takeda.

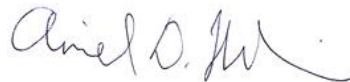
171. I understand that my opinions discussed above support a legal conclusion that claims 1-10 are nonobvious.

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: March 28, 2024

A handwritten signature in blue ink, appearing to read "Aviel D. Rubin", is written over a horizontal line.

Aviel D. Rubin, Ph.D.

EXHIBIT A

Aviel D. Rubin, Ph.D.

Professor Emeritus, Johns Hopkins University
Chief Scientist & Founder, Harbor Labs



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 and joined Harbor Labs, a company he founded in 2011, as Chief Scientist. 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 Monrose, 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 Labs, Founder & Chief Scientist

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

- 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).
- 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 Monroe, 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 Monroe, 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 Monroe 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. Marshall, 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, 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:** 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 Kohnno), 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 18-22, 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:** 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 28/29, 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 Voter Verified 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

- **Proxense, LLC**, vs. Google., Case # 6:23-cv-00320-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent claim construction)
 - Expert Testimony at deposition, Key West, FL (December 18, 2023).
- **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).
- **WSOU Investments, LLC**, vs. Cisco Systems Inc., Case # 6:21-cv-00128-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (March 30, 2023).
 - Expert Testimony at deposition, Annapolis, MD (January 18 & 19, 2023).
- 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, Inv 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 2021, 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 10/11, 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. Invoicea, Inc. and Invoicea 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; Flachsbarth & 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 Monroe, 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

Technical Advisory Boards

Current Positions

Qualytics: Data Quality Assurance

RunSafe: Binary rewriting to protect software

MarinaLife: Online boat slip bookings

Past Technical Advisory Board Positions with Successful Exits

Arbor Networks: Acquired by Danaher, August, 2010.

Authentica: Acquired by EMC Corporation, March, 2006.

Fortify Software: Acquired by Hewlett Packard, September 2010.

Gilian Technologies: Acquired by Breach Security, Inc, July, 2004.

Hx Technologies: Acquired by MEDecision, May, 2009.

Indigo Security: Acquired by Tablus, February, 2005.

NeoPath Networks: Acquired by Cisco, April, 2007.

Netscaler: Acquired Citrix Systems, August, 2005.

SiteAdvisor: Acquired by McAfee, April, 2006.

Tablus: Acquired by EMC Corporation, August, 2007.

ZeroFox: Public Offering via SPAC, July, 2022.