harborexperts

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

SAMSUNG ELECTRONICS CO. LTD., and SAMSUNG ELECTRONICS AMERICA, INC., Petitioners, v. FOUR BATONS WIRELESS, LLC, Patent Owner.	Case No. IPR2025-00495

EXPERT DECLARATION OF DR. AVIEL D. RUBIN ON PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,239,671

Aviel Dr. Rubin

June 23, 2025

CONFIDENTIAL – ATTORNEYS' EYES ONLY

TABLE OF CONTENTS

I. INTRODUCTION....4
A. Background....5
B. Curriculum Vitae....10
C. Materials Considered....10
II. SUMMARY OF OPINIONS....11
III. UNDERSTANDING OF LEGAL PRINCIPLES....12
IV. CLAIM CONSTRUCTION....18
V. TECHNOLOGICAL BACKGROUND....20
A. Wireless Network Access Technologies and Standards....21
a. 802.11 Security Protocols....21
b. Dynamic Keys....23
B. Authentication, Authorization, and Accounting....24
C. Extensible Authentication Protocol (EAP)....26
VI. OVERVIEW OF PATENT NO. 8,239,671....29
VII. OVERVIEW OF PETITIONERS' REFERENCES....34
A. U.S. Patent No. 7,787,627 (Sood) [EX1005]....34
B. Extensible Authentication Protocol (EAP) Key Management Framework (Aboba) [EX1006]....36
C. U.S. Published Patent Application No. 2004/0242228 (Lee) [EX1007]....40
VIII. DR. MANDAYAM FAILS TO SHOW THE CLAIMS OF THE '671 PATENT ARE OBVIOUS IN LIGHT OF THE ALLEGED PRIOR ART....43
A. Ground 1 Fails to Show Claims 1-4, 7, 8, 12, 14, and 16 of the '671 Patent are Obvious Over Sood....43
a. Claim 1....44
i. 1[a]: "cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods;"....44
ii. 1[b]: "further including deriving a channel binding key from a channel binding master key bound to a key binding blob using a key derivation function; and"....52
1. Dr. Mandayam's First Mapping Fails....54
2. Dr. Mandayam's Second Mapping Fails....56

3. Dr. Mandayam's Third Mapping Fails....58
iii. 1[c]: "wherein said key binding blob is a string that is constructed from static parameters advertised from an authenticator."....60
b. Claim 2: "The method of claim 1, wherein said authentication methods include EAP methods."....63
c. Claim 3: "The method of claim 1, wherein said parameters include parameters advertised by an authenticator to said supplicant."....63
d. Claim 4: "The method of claim 3, wherein the identity of the authenticator is one of said parameters."....64
e. Claim 7: "The method of claim 1, wherein said key binding blob is an octet-string that is constructed from static parameters advertised from an authenticator using an authenticator-supplicant protocol."....64
f. Claim 8: "The method of claim 1, including a network side authenticator and said supplicant using the channel binding master key for protecting an authenticator-supplicant protocol."....64
g. Claim 12: "The method of claim 1, further including creating multiple channel binding keys from a single channel binding master key for multiple authenticators."....65
h. Claims 14, 16: "The method of claim [1/12], further including creating multiple channel binding keys from a single channel binding master key for multiple authenticators using different key binding blobs for different authenticators."....65
B. Ground 2 Fails to Show Claims 5 and 18 of the '671 Patent are Obvious Over the Combination of Sood and Aboba....66
a. Claim 5: "The method of claim 1, wherein said channel binding master key is at least 64 octets long."....66
b. Claim 18: "The method of claim 1, wherein said key derivation function is computed based on CBK=kdf+(CBMK, KBB), where CBK represents channel binding key, CBMK represents channel binding master key, and KBB represents key binding blob."....67
C. Ground 3 Fails to Show Claims 6, 10, 11, 13, 15, 17, and 19 of the '671 Patent are Obvious Over the Combination of Sood and Lee....67
a. Claim 6....68
i. 6[a]: "using an extensible authentication protocol server to cryptographically bind access network parameters to a channel binding key

and to transmit said channel binding key to an extensible authentication protocol authenticator for use by the extensible authentication protocol authenticator as an extensible authentication protocol master session key without said extensible authentication protocol authenticator needing to carry said access network parameters in extensible authentication protocol authentication methods;” 68

ii. 6[b]: “including using said extensible authentication protocol server to derive said channel binding key from a channel binding master key bound to a key binding blob using a key derivation function;” 69

iii. 6[c]: “wherein said key binding blob is a string that is constructed from static parameters advertised from said extensible authentication protocol authenticator.” 69

b. Claim 10: “The method of claim 1, further including that: a) a server and the supplicant create a channel binding key used for an authenticator; b) the server transfers the channel binding key to the authenticator; and c) the supplicant and the authenticator verify proof of possession of the channel binding key over an authenticator-supplicant protocol.”.....70

c. Claim 11: “The method of claim 10, further including that the channel binding key is derived from a channel binding master key bound to a key binding blob associated with the authenticator using a key derivation function.”.....71

d. Claims 13, 15, 17: “The method of claim [12/14/16], further including using channel binding keys to form a hierarchical channel binding.”.....71

e. Claim 19: “The method of claim 3, wherein said authenticator is an EAP authenticator, and wherein the EAP authenticator receives and processes the channel binding key as a Master Session Key (MSK).”.....72

D. Ground 4 Fails to Show Claims 1-8 and 10-19 of the ’671 Patent are Obvious Over the Combination of Sood, Aboba, and Lee.....72

a. “without needing to carry the parameters in authentication methods” / “without … needing to carry said access network parameters in … authentication methods”.....73

IX. CONCLUSION.....74

I. INTRODUCTION

1. My name is Aviel D. Rubin, Ph.D. I have been retained by Batons, LLC ("Four Batons") through its counsel, Heim, Payne & Chorush, LLP, as an independent expert witness in IPR 2025-00495.

2. The company for which I work, Harbor Experts, is being compensated at the rate of $975 per hour for the time that I spend on this case. Harbor Experts is also being reimbursed for my reasonable and customary expenses. Members of the staff at Harbor Experts have worked at my direction and under my supervision to assist me in this engagement. Neither I nor Harbor Experts have received any additional compensation for my work on this case. My and Harbor Experts' compensation is not dependent in any way on the contents of this Declaration, the substance of my testimony, or the results of this lawsuit.

3. I have been asked by counsel for Four Batons to provide my independent technical expert opinion on subjects relevant to this IPR. I have reached my opinions based on my review of facts and materials relevant to this matter. This expert declaration ("Declaration") contains statements of my opinions formed to date and the bases and reasons for those opinions. All opinions and facts stated in this Declaration are true and correct to the best of my knowledge. If called upon to testify, I could and would testify to the substance, contents, reasons, and bases for the statements and opinions in this Declaration and any supplemental declarations

that I may prepare in connection with the above-captioned matter. I reserve the right to supplement my opinions and offer additional opinions based on further review of materials in this case, including opinions and/or information of other expert witnesses and/or relevant documents and information that are produced after the date of this Declaration.

A. Background

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:

12. 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;

13. In 2010, I received a Fulbright Scholarship to serve as a Visiting Professor at Tel Aviv University in Israel;

14. In 2009, I received a Google Research Award for my work on securing medical records on smartphones;

15. 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;

16. In 2004, I was named Baltimorean of the Year by Baltimore Magazine for my work in safeguarding the election process;

17. In 2004, I received the Electronic Frontiers Foundation Pioneer Award; and

18. In 2000, I received the Best Paper Award at the 9th USENIX Security Symposium.

19. 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.

20. 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.

21. 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").

22. A detailed record of my professional qualifications is set forth in the attached Appendix 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.

23. 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 declaration.

24. 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.

B. Curriculum Vitae

25. Additional details of my education and employment history, recent professional service, patents, publications, and other testimony are set forth in my current curriculum vitae, attached to this declaration as Appendix A.

C. Materials Considered

26. In forming my opinions in this Declaration, I have considered and may rely upon my own personal knowledge, education, and many years of experience

relating to computer science and security, as well as my review of Petitioner's filing and all associated materials in this matter and relevant technical and academic literature and other publicly available evidence. The documents and materials I have considered or relied upon are cited in the body and footnotes of this Declaration.

27. I may rely upon these materials and/or additional materials to rebut arguments raised by Petitioner, or to respond to witness testimony that has not yet been given. Further, I reserve the right to review and consider other information and materials throughout these proceedings, including any other documents or testimony that may emerge in these proceedings. Those materials may affect my opinions in this matter. I further reserve the right to rely on uncited portions of the publications I identify in this Declaration, other publications, and other testimony, including expert testimony.

II. SUMMARY OF OPINIONS

28. It is my opinion that Dr. Mandayam has failed to show the grounds for challenge set forth by the Petitioners demonstrate that any of the claims of '671 Patent are not patentable over the alleged prior art. Specifically, Dr. Mandayam does not show any of the following grounds for challenge are valid:

29. **Ground 1:** Challenges claims 1-4, 7, 8, 12, 14, and 16 as obvious over Sood. The '671 claims are not invalidated under Ground 1.

30. **Ground 2:** Challenges claims 5 and 18 as obvious over the combination of Sood and Aboba. The '671 claims are not invalidated under Ground 2.

31. **Ground 3:** Challenges claims 6, 10, 11, 13, 15, 17, and 19 as obvious over the combination of Sood and Lee. The '671 claims are not invalidated under Ground 3.

32. **Ground 4:** Challenges claims 1-8 and 10-19 as obvious over the combination of Sood, Aboba, and Lee. The '671 claims are not invalidated under Ground 4.

33. My reasoning and evidence for these opinions are provided in Section IX of my declaration.

III. UNDERSTANDING OF LEGAL PRINCIPLES

34. I am not an attorney. In forming my opinions in this case, I used the following legal standards that were explained to me by counsel.

35. An IPR should not be instituted unless Petitioners have shown a likelihood of success on the invalidity grounds presented in the petition. *See In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) ("[T]he Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.").

36. "In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid*

Tech., Inc., 815 F.3d 1356, 1363 (Fed. Cir. 2016) (petitions must identify "with particularity… the evidence that supports the grounds for the challenge to each claim"); 35 U.S.C. § 312(a)(3). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

37. "To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness." *In re Magnum Oil Tools*, 829 F.3d at 1380. The obviousness inquiry requires considering whether one of skill in the art "would have been motivated to combine the prior art to achieve the claimed invention." *In re NuVasive, Inc.*, 842 F.3d 1376, 1381 (Fed. Cir. 2016) (quoting In re *Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016)). "[T]he factual inquiry whether to combine references must be thorough and searching…" *Id.*

38. **Claim Construction**. I understand that, in an *inter partes* review, claims are construed according to *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). That is, claims are construed as they would be understood to a person of skill in the art at the time of the claimed invention after having considered the intrinsic and extrinsic evidence, including the claims, specification, and file history.

39. **Obviousness**. I understand that the relevant standard for obviousness (found at 35 U.S.C. § 103, pre-AIA) is as follows:

> A patent for a claimed invention may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

40. Thus, Patent challengers may show that a claim is invalid for obviousness under 35 U.S.C. § 103 if they demonstrate that two or more prior art references in combination disclose, expressly or inherently, every claim limitation so as to render the claim, as a whole, obvious. Alternatively, patent challengers may show that a claim is invalid for obviousness under 35 U.S.C. § 103 if a single prior art reference combined with the knowledge of one of ordinary skill in the art discloses every claim limitation so as to render the claim, as a whole, obvious.

41. It is my understanding that in assessing the obviousness of claimed subject matter, one should evaluate obviousness over the prior art from the perspective of one of ordinary skill in the art at the time that invention was made

(and not from the perspective of either a layman or a genius in that art). The question of obviousness is to be determined based on:

- The scope and content of the prior art;
- The difference or differences between the subject matter of the claim and the prior art (whereby in assessing the possibility of obviousness one should consider the manner in which a patentee and/or a Court has construed the scope of a claim);
- The level of ordinary skill in the art at the time of the alleged invention of the subject matter of the claim; and,
- Any relevant objective factors (the "secondary considerations") indicating nonobviousness.

42. It is also my understanding that the United States Supreme Court clarified the law of obviousness in *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. at 398 and 419 (2007). It is my understanding that to determine whether it would have been obvious to combine known elements in a manner claimed in a patent, one may consider such things as that interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, and the background knowledge of one with ordinary skill in the art. The secondary considerations at issue may include commercial success of a product using the invention, if that commercial success is due to the invention; long-felt need for the

invention; evidence of copying of the claimed invention; industry acceptance; initial skepticism; failure of others; and praise of the invention.

43. I also understand that, while an analysis of any teaching, suggestion, or motivation to combine elements from different prior art references is useful in an obviousness analysis, the overall inquiry must be expansive and flexible.

44. I further understand that it is impermissible to use a hindsight reconstruction of references to reach the claimed invention without any explanation as to how or why the references would be combined to produce the claimed invention.

45. Moreover, I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. But multiple prior art references or elements may, in some circumstances, be combined to render a patent claim obvious. I understand that I should consider whether there is an "apparent reason" to combine the prior art references or elements in the way the claimed invention does. Requiring a reason for the prior art combination protects against distortion caused by hindsight. Along the same lines, one cannot use the challenged patent as a blueprint to piece together the prior art in order to combine the right ones in the right way as to create the claimed inventions.

46. To determine whether there is such an "apparent reason" to combine the prior art references or elements in the way that a challenged claim does, it may be necessary to look to the interrelated teaching of multiple references, to the effects of demands know to the design community or present in the marketplace, and to the background knowledge possessed by a person having ordinary skill in the art.

47. I also understand that when the prior art teaches away from combining prior art references or certain known elements, discovery of a successful means of combining them is more likely to be non-obvious. A prior art reference may be said to teach away from a claim when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the claim or would be led in a direction divergent from the path that was taken by the claim. Additionally, a prior art reference may teach away from a claimed invention when substituting an element within that prior art reference for a claim element would render the claimed invention inoperable.

48. I understand that, in order to be considered as "prior art" for purposes of the § 103 obviousness inquiry, a reference must be "analogous" to the Asserted Patents. I understand that a reference is "analogous" if (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention).

49. **Person Of Skill In The Art.** When interpreting a patent, I understand that it is important to view the disclosure and claims of that patent from the level of a person of ordinary skill in the relevant art (a "POSITA") at the time of the invention. In determining the level of ordinary skill in the art, one should consider:

- The level of education and experience of persons actively working in the above fields at the time the subject matter at issue was developed;
- The types of problems encountered in the art at the time the subject matter was developed;
- The rapidity with which innovations are made in those fields;
- Prior art patents and publications;
- Prior art solutions to the problems addressed by the relevant art; and
- The sophistication of the technology at issue in this case.

IV. CLAIM CONSTRUCTION

50. In the parallel district court proceeding, I understand that the same parties agreed to the following constructions for the '671 Patent:

Claim Language	**Agreed Construction**
"channel binding key" ('671 Patent, claims 1, 6, 10, 11, 18, 19)	"a key that is derived from a Channel Binding Master Key and cryptographically bound to a Key Binding Blob using a Key Derivation Function"

“channel binding master key” (’671 Patent, claims 1, 6, 8, 11, 18)	“a key from which a Channel Binding Key is derived using a Key Derivation Function”
“key binding blob” (’671 Patent, claims 1, 6, 8, 11, 18)	“an octet-string that is constructed from static parameters advertised from an authenticator using an Authenticator-Supplicant Protocol”
“authenticator” (’671 Patent, claims 1, 3, 4, 7, 10, 11, 19)	“a network-side entity that uses a Channel Binding Key for an Authenticator-Supplicant Protocol”
“supplicant” / “mobile supplicant” (’671 Patent, claims 1, 3, 8, 10)	“a user-side entity that uses a Channel Binding Key for an Authenticator-Supplicant Protocol”
“authenticator-supplicant protocol” (’671 Patent, claims 7, 8, 10)	“a protocol that is executed between a supplicant and an authenticator and uses a Channel Binding Key for protecting the protocol”
“[deriving a / derive said] channel binding key from a channel binding master key bound to a key binding blob using a key derivation function” (’671 Patent, claims 1, 6)	“[deriving a / derive said] channel binding key from a channel binding master key and binding the channel binding key to a key binding blob using a key derivation function”
“said parameters” (’671 Patent, claims 3, 4)	“said access network parameters”
“said supplicant using the channel binding master key for protecting an authenticator-supplicant protocol” (’671 Patent, claim 8)	Plain and ordinary meaning

51. Dr. Mandayam appears to agree with these constructions, too. *See* Mandayam Report at ¶¶ 61-67. For purposes of this Declaration, I have applied these constructions in my analysis.

52. However, in the parallel district court litigation, I understand the parties dispute the constructions of the following terms from the '671 Patent:

Claim Language	Patent Owner Construction	Petitioners Construction
"server" ('671 Patent, claim 10)	Plain and ordinary meaning	"An entity that creates a CBK and transfers it to the authenticator. A server is a creator as well as a sender of the CBK."
"EAP methods" ('671 Patent, claim 2)	Plain and ordinary meaning	"the authentication algorithms described in RFC 3748"

53. The constructions of these disputed terms do not matter for purposes of this Preliminary Response, however, since I do not distinguish the prior art on the basis of these disputed terms.

V. TECHNOLOGICAL BACKGROUND

54. The '671 Patent has its background in systems and devices that facilitate secure wireless access to computer networks using an authentication framework that separates the access point (authenticator) from the backend authentication server. The technology helps users connect safely to wireless

networks by managing how devices prove their identity before gaining access. Instead of making security decisions at the access point, the system forwards authentication messages to a central server that makes the decision. This is accomplished using the Extensible Authentication Protocol (EAP), a standard protocol for secure and flexible network authentication.

A. Wireless Network Access Technologies and Standards

55. At the time of the priority date of the ’671 Patent, in April 2006, wireless networking technologies had become well established and widely adopted. The IEEE 802.11 standards, commonly known as Wi-Fi, had been developed and standardized to enable wireless communication between devices over local area networks. Early versions of these standards, such as 802.11a, 802.11b, and 802.11g, defined the technical protocols for transmitting data over radio frequencies, allowing devices like laptops, personal digital assistants (PDAs), and other wireless-enabled equipment to connect without physical cables.

a. 802.11 Security Protocols

56. Security has been at the forefront of wireless communications for decades. Because of the nature of having to communicate wirelessly between end-devices and network entities (i.e., the air interface), this exposes communications to various attack vectors that would otherwise not be a concern (e.g., wireless eavesdropping). As such, security has been an ongoing problem of wireless

communications, which has continued to grow in importance with the prevalence of wirelessly connected devices.

57. Security features were first accounted for in the original 802.11 standard when it was ratified in 1997, which introduced the Wired Equivalent Privacy (WEP) protocol. However, this protocol was relatively simple by modern standards and possessed many security vulnerabilities, which led to its obsolescence. Possibly the greatest deficiency in the WEP protocol was its use of static keys. As such, this was addressed in the protocols that would replace it.

58. The 802.11g standard, which was released in 2003, defined the Wi-Fi Protected Access (WPA) protocol. WPA was introduced as an intermediate measure to provide temporary relief to the security concerns with WEP, until a more formalized version could be added to the standard. WPA introduced dynamic keys, which is a concept that is an essential part of WPA itself, as well as the later revisions to WPA. This concept appears in WPA2, which was released in the 2004 standard 802.11i as the formalized/revised version of WPA. While used in a different way compared to its predecessors, the modern WPA3 protocol (introduced as a security certification to enhance the security features of existing standards, particularly 802.11x) still makes use of dynamic keys as well.

59. Security was a critical concern for wireless networks. WPA2 was the primary encryption and access control protocol used to protect Wi-Fi

communications in 2006. WPA2's definitions are embodied in 802.11i. As networks grew and complexity—especially in corporate and campus settings—WPA2's centralized authentication needed extension. WPA3 later improved on this foundation, adding stronger encryption and protections against password-guessing attacks.

b. Dynamic Keys

60. WPA and WPA2 make use of the concept of dynamic keys. This is an integral part of the security benefits the protocols provide that was not present in the previous WEP protocol. The concept of dynamic keys is to derive, establish, and make use of cryptographic keys that are frequently changed or rotated. This enhances security by limiting the impact of a key compromise and makes compromise overall more challenging for an adversary. However, establishing dynamic keys requires more clever schemes compared to static keys and needs to be done in a secure manner that allows only specific parties to perform key derivation.

61. In WPA and WPA2, this is accomplished by what is known as a four-way handshake. The four-way handshake is the process of exchanging 4 messages between an access point (authenticator) and the client device (supplicant) to generate encryption keys that can be used to encrypt actual data sent over a wireless medium. The goal of the four messages is to generate a key used to encrypt all unicast traffic between a client station and the access point, often called a Pairwise Transient Key

(PTK), securely using other keys and keying information. Provided here is a diagram of the general-purpose four-way handshake messaging flow used in WPA2 that is defined in the 802.11i standard:

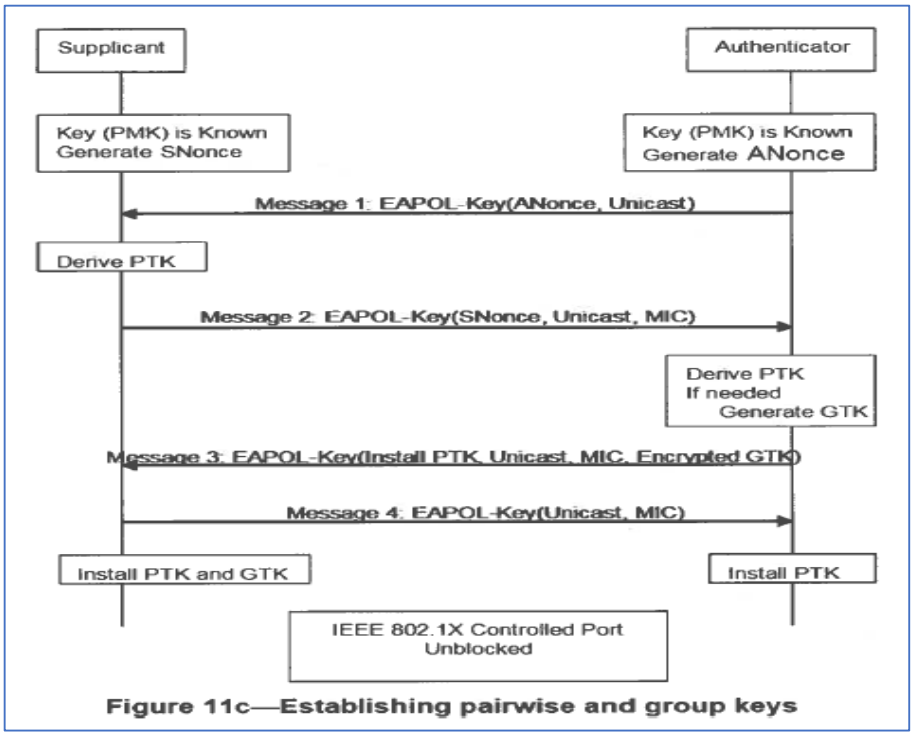


Figure 11c—Establishing pairwise and group keys

EX1009 (IEEE802.11i) at 31

B. Authentication, Authorization, and Accounting

62. In enterprise deployments, wireless authentication often uses the RADIUS protocol to relay Extensible Authentication Protocol (EAP) messages between access points and backend servers. RADIUS is an authentication, authorization, and accounting (AAA) protocol that is defined in the IEEE 802.1X and IETF standards. RADIUS-enabled access points forward login credentials and authentication information securely, allowing centralized decision-making rather

than local processing at each access point. While it still sees use today, RADIUS was later improved upon by the Diameter protocol, which offers more advanced security features and is widely used in both modern IP-based networks and cellular networks.

63. Despite this setup offered by RADIUS, many legacy access points still performed local authentication or had limited support for enforcing centralized policies. This led to inconsistent security, harder management, and difficulties updating authentication methods across the network, such as deploying new credential types like digital certificates.

64. The Extensible Authentication Protocol (EAP) provided a flexible framework that supported multiple authentication methods—including passwords, certificates, and tokens—within RADIUS-based enterprise Wi-Fi. Nonetheless, the lack of clear separation between authentication decisions (made by the server) and enforcement points (the access point) presented challenges in scalability and security policy control.

65. The ’671 Patent introduced a new system related to these limitations. By formalizing the separation of roles—where the access point relays authentication, and the backend server makes decisions via EAP over RADIUS—the invention enabled centralized, scalable authentication. This architecture improved consistency, streamlined security administration, and enhanced the ability to support

diverse authentication methods in large wireless networks. This is further described in Section VII of my report.

C. Extensible Authentication Protocol (EAP)

66. At the time of the priority date of the ’671 Patent, in April 2006, organizations and users increasingly relied on Wi-Fi networks for accessing private and public data services. While the IEEE 802.11 standards had already provided a well-established framework for wireless networking, security remained a critical concern—particularly in enterprise and multi-user environments where verifying a user’s identity before granting access to the network was essential. The growing demand for secure and scalable access control mechanisms gave rise to several technologies, one of which was the Extensible Authentication Protocol (EAP). Originally standardized in RFC 2284 and later updated in RFC 3748, EAP was designed as a flexible authentication framework that supported a wide range of authentication methods across various network types.

67. EAP’s major strength lies in its flexibility and extensibility. Unlike traditional protocols that embedded fixed credential checks into network hardware, EAP allowed for the separation of roles and responsibilities: an access point or switch could act merely as a relay (an “authenticator”), while a backend server, such as a RADIUS server, performed the actual authentication. This separation was particularly important in environments like universities, enterprises, and public

hotspots, where centralized user credential management was needed. EAP was intentionally designed to be media-agnostic and protocol-independent, supporting wireless, wired, and other access technologies. Through integration with 802.1X and WPA2/WPA3 enterprise standards, EAP became a cornerstone of secure wireless access.

68. The design of EAP emphasized several technical principles—or "invariants"—that made it adaptable and robust across different contexts. These included media independence (EAP could operate over wireless or wired media without changes), mode independence (EAP functioned regardless of whether authentication was local or remote), and method independence (authenticators didn't need to understand or implement specific authentication mechanisms). These principles enabled EAP to support various authentication methods, including EAP-TLS (certificate-based), EAP-TTLS (tunneled), and EAP-PEAP (protected password-based), while remaining agnostic to the underlying cryptographic choices.

69. EAP's use in 802.11 networks depended on a tri-party architecture involving a supplicant (the client device), an authenticator (usually a wireless access point), and a backend authentication server. The authenticator acted as a pass-through device, forwarding EAP messages between the client and the authentication server. This setup enabled the central server to make informed decisions about access, while the access point focused on enforcing the results of that decision. In

large-scale deployments, virtual access points or virtual authenticators could be used to manage multiple logical networks over a single piece of physical hardware, each isolated for security purposes.

70. However, despite the flexibility of the protocol, implementing secure key management and maintaining the proper lifecycle of cryptographic material were complex challenges. The generation of keying material—especially pairwise master keys (PMKs) and session keys—needed to be handled with strong entropy and proper cryptographic practices. The protocol itself did not dictate re-keying or key expiration logic, so these responsibilities were often delegated to the surrounding infrastructure. Moreover, certain advanced use cases, such as roaming or fast reauthentication, required the correct implementation of key hierarchies and parent-child key relationships. If parent keys were not invalidated or regenerated appropriately, it risked undermining the security assurances provided by EAP.

71. These complexities, along with growing pressure to simplify wireless access across many access points and client types, created challenges for product developers and network administrators alike. The inventors of the ’671 Patent proposed a technical solution that addressed these challenges, including how authenticators—whether virtual or physical—could securely and independently perform their role in the EAP process. The claimed invention offered methods for managing state, exchanging keys, and handling authenticator behavior in a way that

maintained protocol compliance while reducing security risks. The patent therefore addressed specific implementation gaps in EAP-based systems that were not fully resolved by the existing standards alone.

VI. OVERVIEW OF PATENT NO. 8,239,671

72. The ’671 Patent is entitled, “Channel binding mechanism based on parameter binding in key derivation.” It was filed on April 20, 2006, and issued on August 7, 2012, as U.S. Patent No. 8,239,671 B2.

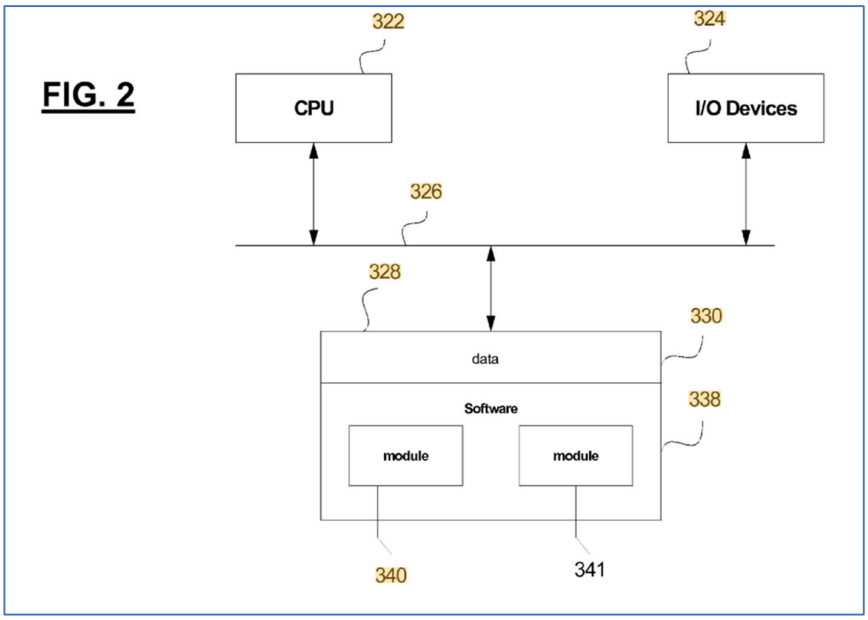
73. The ’671 Patent pertains to a method for strengthening authentication in wireless and other access networks, particularly those using the Extensible Authentication Protocol (EAP). ’671 Patent, Abstract. The invention enhances trust between a mobile supplicant (e.g., a client device) and an access network by cryptographically binding access network parameters (e.g., the identity of an access point or other authenticators) to a key derived during authentication. A person of ordinary skill in the art would understand that this feature helps ensure that a client device does not merely authenticate to a central server, but can also confirm that it is interacting with the correct access network element, thereby mitigating threats such as rogue authenticators or man-in-the-middle attacks.

74. The ’671 Patent addresses these concerns by introducing a mechanism whereby access network parameters are not nakedly transmitted as part of the EAP authentication exchange, but are instead embedded in the cryptographic keying

material derived during the process. For example, independent Claim 1 of the ’671 Patent describes a method for performing channel binding by cryptographically binding access network parameters—such as static information broadcast by an access point—to a key using a key derivation function. ’671 Patent, claim 1.

75. The invention disclosed in the ’671 Patent is novel in its approach to cryptographically binding access network parameters to session keys without transmitting those parameters through the authentication method itself. Prior to this invention, existing EAP-based authentication methods often required explicit transmission or verification of network identifiers, which introduced security risks such as man-in-the-middle attacks and rogue access points. The ’671 Patent departs from these conventional approaches by deriving a channel binding key (CBK) from both a channel binding master key (CBMK) and a key binding blob (KBB) that is constructed from static network parameters. The KBB is a string constructed from static parameters advertised by the authenticator (e.g., a network access point), such as its identity or role. This technique ensures that the authenticator's identity and other network information are embedded within the key material itself, providing implicit verification and a cryptographically enforced trust relationship—an inventive step that eliminates the need to transmit sensitive parameters and enhances both security and protocol efficiency.

76. As shown in Figure 2, the system may be implemented using a computing platform that includes a central processing unit (CPU), memory, and I/O modules. These components can perform the key derivation functions and handle the exchange of keys and authentication data between the supplicant, authenticator, and authentication server.



'671 Patent, Fig. 2, 8:5–9:4.

77. The '671 claims further specify the context and usage of this mechanism. For instance, claim 2 indicates that the authentication methods include EAP methods, and Claim 3 clarifies that the parameters include those advertised by an authenticator to the supplicant. Claim 5 adds that the channel binding master key (CBMK) is at least 64 octets long.

78. Claim 6 of the ’671 Patent describes a system implementation where an EAP server performs the derivation and then provides the resulting CBK to the authenticator. The CBK can be used directly as a Master Session Key (MSK), allowing the authenticator to participate in the secure session without needing to receive or verify the access network parameters independently. ’671 Patent, claim 6. This facilitates a secure transfer of trust from the authentication server to the authenticator.

79. The system further allows the authentication server to send the derived CBK to an authenticator without exposing sensitive access network identifiers over the wire, thereby maintaining both security and efficiency. Claim 7 explains that the key binding blob (KBB) may be constructed as an octet-string. Claims 8 and 9 indicate that the CBMK may also be used to protect communication over an authenticator-supplicant protocol, and that the supplicant may obtain the KBB using such a protocol.

80. Claims 10 and 11 describe the process by which both the supplicant and the authenticator prove possession of the same derived key (CBK), thus establishing mutual trust. In this method, the supplicant and the authentication server derive a CBK, the server sends the key to the authenticator, and both ends verify possession over the channel.

81. Claims 12 through 17 extend the invention to multi-authenticator environments, where multiple CBKs may be derived from a single CBMK using different key binding blobs. This enables a hierarchical channel binding structure, as depicted in Figure 4, in which secure relationships may be maintained across multiple authenticators or layers of a network infrastructure.

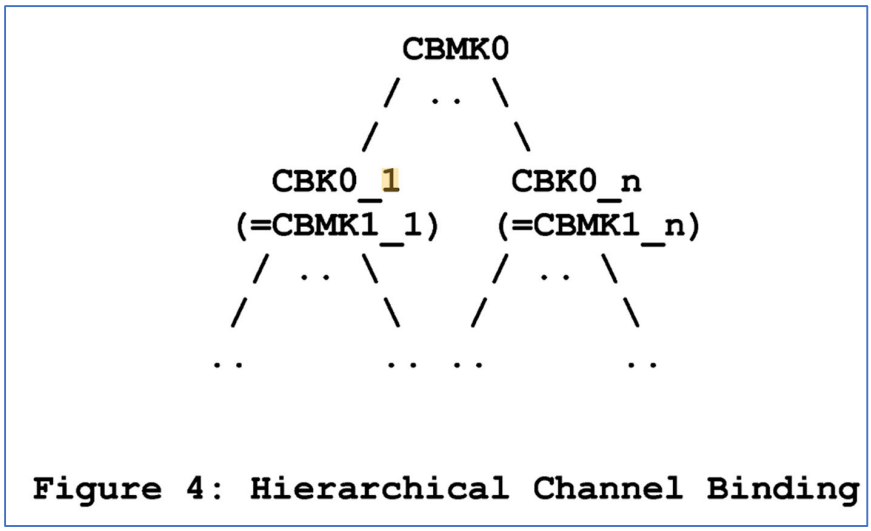


Figure 4: Hierarchical Channel Binding

'671 Patent, Fig. 4, 11:14–12:5.

82. Claim 18 presents the mathematical formulation of the key derivation: CBK = kdf + (CBMK, KBB). This formula captures the essence of the invention—deriving a key that is cryptographically bound to network parameters, without requiring those parameters to be sent as part of the authentication protocol.

83. Finally, claim 20 recites an authentication server configured to perform the method described above. The server receives a KBB from the authenticator, uses it together with a CBMK to derive the CBK, and then provides the resulting key to

the authenticator for use as a master session key—without ever transmitting the network-identifying parameters over the EAP channel. Claim 21 specifies that the authentication server may be an EAP server.

VII. OVERVIEW OF PETITIONERS' REFERENCES

A. U.S. Patent No. 7,787,627 (Sood) [EX1005]

84. The US 7787627B2 Patent ("Sood") is entitled "Methods and apparatus for key management in wireless communication networks." Sood was filed on Nov. 30, 2005.

85. Sood's main objective is to provide methods and apparatus "for providing a key management system for wireless communication networks." Sood at Abstract. In particular, the invention addresses the challenge of reducing latency and preserving security during wireless handoffs between different access points (APs) by managing cryptographic key material in a way that balances speed and protection against compromise. Sood at [0003]-[0006].

86. The patent explains that in conventional systems, full re-authentication during handoffs between APs can introduce unacceptable delays. A simplistic solution might involve sharing a master key among APs, but this increases security risk—if one AP is compromised, the entire network is at risk. Sood at [0004]-[0005].

87. To solve this, Sood provides two primary approaches to key management: a distributed key management architecture and a centralized key

management architecture. In both cases, temporary keys are derived for each AP to which a mobile terminal (MT) might connect, without requiring full re-authentication or exposing the master key. Sood at [0006]-[0009].

88. In the distributed architecture, the current AP (referred to as AP_1) derives a temporary key for a neighboring AP (AP_2) using a master key (MK) and AP_2's unique identifier (e.g., its MAC address). AP_1 then sends the derived key to AP_2, while the MT independently computes the same key using the same derivation function and AP_2's identifier. This allows the MT to transition to AP_2 securely and quickly without repeating the full authentication process. Sood at [0010]-[0013]; [0045]-[0050].

89. Figure 8 of Sood illustrates one way a communication node (e.g., an access point) can be configured to implement this key management system. See Sood at Fig. 8. In this implementation, a communication node (e.g., access point 230 in Fig. 2) receives a master session key (MSK) from an authentication server after a mutual authentication process (block 810). It then derives a first-level authentication key (e.g., PMK-R0), generates a key name (block 830), and subsequently derives one or more second-level keys (e.g., PMK-R1) for neighboring APs (block 840). These second-level keys are assigned to APs the mobile device may roam to—e.g., PMK-R1-1 remains local, while PMK-R1-2 and PMK-R1-3 are securely forwarded to APs 240 and 250, respectively (block 860). This structure supports fast, secure

roaming by ensuring each AP already holds a valid session key before the mobile terminal arrives. Sood at [0066]-[0070].

90. In an alternative embodiment, Sood describes a centralized key management architecture where a trusted server—referred to as an Authenticator—generates and distributes temporary keys for each AP. In this setup, the Authenticator computes temporary keys using the MK and AP identifiers and securely distributes the key to both the MT and the relevant APs. This architecture offloads key computation from the APs, which may be beneficial for scalability and control. Sood at [0014]; [0055]-[0060]. Temporary keys are proactively generated and distributed only to these APs, which balances computational efficiency with readiness for mobility. Sood at [0030]; [0061]-[0064].

B. Extensible Authentication Protocol (EAP) Key Management Framework (Aboba) [EX1006]

91. The RFC 3748 specification ("Aboba") is entitled *"Extensible Authentication Protocol (EAP)."* Aboba was published in June 2004 by Bernard Aboba, Larry Blunk, John Vollbrecht, James Carlson, and Henrik Levkowetz, and it obsoletes the earlier RFC 2284.

92. Aboba's main objective is to define a "general protocol for PPP authentication that supports multiple authentication mechanisms." Aboba at Abstract. More broadly, EAP provides an extensible framework that supports a

variety of authentication methods across different types of network links, including wireless (IEEE 802.11), wired (IEEE 802.1X), and point-to-point (PPP) systems. By decoupling authentication mechanisms from the transport, EAP allows diverse, multi-step authentication exchanges to occur over existing network infrastructure.

93. EAP operates in a lock-step exchange between three functional entities: the Supplicant (e.g., user device), the Authenticator (e.g., wireless access point or switch), and the Authentication Server (e.g., RADIUS server). The Authenticator relays messages between the Supplicant and Server without interpreting the content. Aboba at §1.1. The protocol consists of a small set of message types: Request, Response, Success, and Failure, which are used to carry method-specific authentication data.

94. EAP is a method-independent protocol. That means it acts as a container framework for specific authentication methods (such as EAP-TLS, EAP-MD5, EAP-SIM, etc.), allowing a common exchange format regardless of the authentication type. The method negotiation occurs dynamically between the peer and the authenticator, with support for fallback if an EAP method is not mutually supported. Aboba at §1.2–1.3, §4.

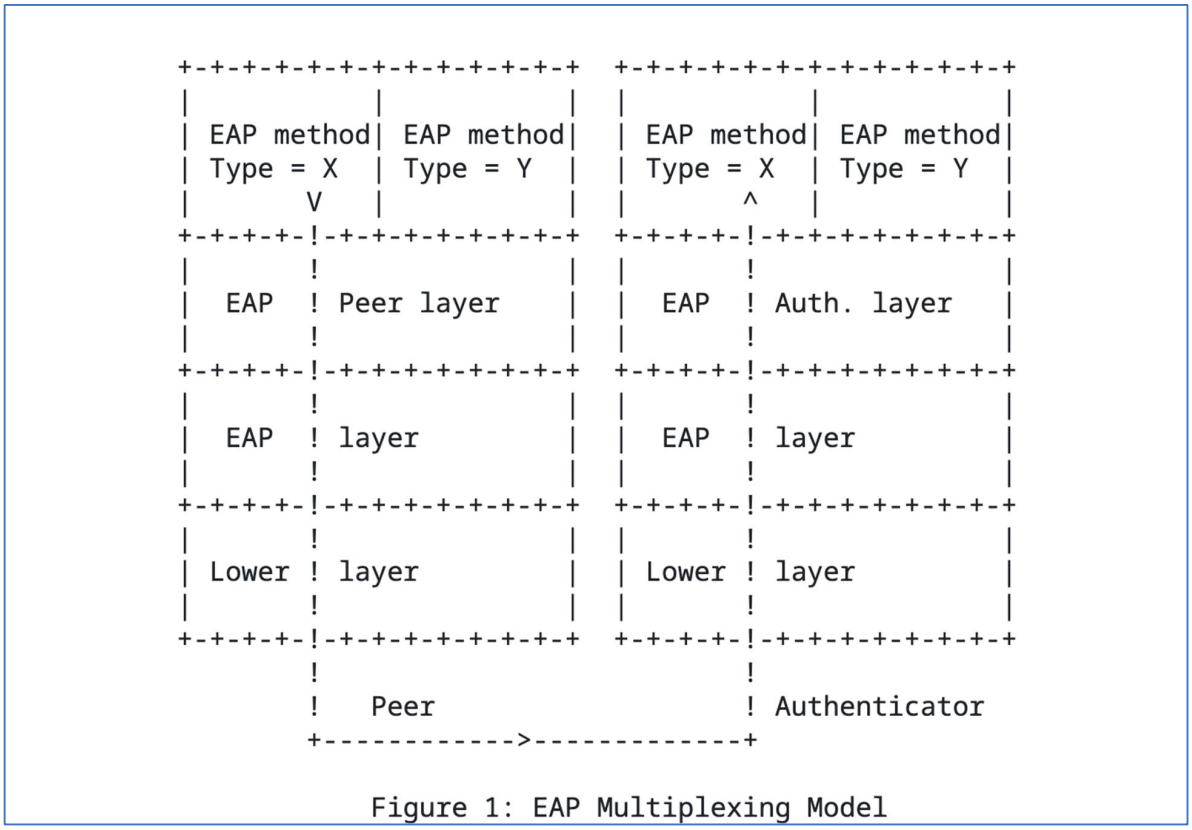


Figure 1: EAP Multiplexing Model

95. A central architectural insight into EAP is illustrated in Figure 1 of the RFC, entitled "EAP Multiplexing Model." *See* Aboba at Fig. 1. This figure is critical for understanding how EAP logically separates EAP methods, EAP layer, and lower layers (e.g., PPP, IEEE 802). At the bottom, the Lower Layer (e.g., PPP or 802.1X) provides transport for EAP messages. Above it, the EAP layer acts as a multiplexer and demultiplexer—it receives EAP packets from the lower layer and directs them to the correct EAP method. The EAP Method Layer contains the actual authentication methods (like EAP-TLS or EAP-MD5), each of which performs the detailed credential exchanges. This model allows EAP to support multiple

authentication methods without modifying the lower-layer protocols, making it highly adaptable across different technologies. The figure also helps visualize how new methods can be added modularly, enhancing security or functionality without altering the transport infrastructure.

96. EAP's separation of concerns allows it to be used flexibly in protocols such as PPP and IEEE 802.1X. In enterprise wireless networks, for example, EAP is often encapsulated in EAPOL (EAP over LAN) and relayed over RADIUS to an authentication server, enabling dynamic credential checking before granting access to the network. Aboba at §1.3, §7.1.

97. Although EAP itself does not provide encryption or integrity protection, it is typically used with secure authentication methods like EAP-TLS or EAP-PEAP that do. EAP assumes that reliability, ordering, and fragmentation are handled by the underlying transport protocol. Aboba at §7.2–7.3.

98. The RFC 3748 framework has served as the basis for a wide variety of standardized and vendor-specific EAP methods. It continues to underpin modern authentication deployments across Wi-Fi, VPNs, wired LANs, and mobile networks, offering a flexible and modular authentication substrate.

C. U.S. Published Patent Application No. 2004/0242228 (Lee) [EX1007]

99. The US 2004/0242228 A1 Patent ("Lee") is entitled "Method for fast roaming in a wireless network." Lee was filed on Jan. 8, 2004 to provisional application No. 60/439,891 (filed on Jan. 14, 2003).

100. Lee's main objective is to provide "[a] roaming service method for a fast and secure wireless network is provided." Lee at Abstract. In Wi-Fi networks, "roaming" happens when a wireless station (STA, like a phone, a laptop, etc. that can connect to a network) moves out of range of one access point (AP) and needs to connect to a neighboring AP. Therefore, Lee provides a set of mechanisms that enables a wireless client device to move between different APs in a wireless network without losing connectivity.

101. Lee's invention is based on a typical infrastructure of Wireless Local Area Networks (WLAN). As I discussed above, Wi-Fi is a particular standard for implementing WLANs based on the IEEE 802.11 standards. As identified by Lee, its invention relies on APs and STAs within the infrastructure. Lee at [0006].

102. Lee discusses the transmission of "proactive keys." According to Lee, proactive keys are cryptographic keys that are pre-generated and pre-distributed to APs that an STA is likely to roam to. These keys are derived from existing authentication information (which I discuss below) and allow the STA to quickly reauthenticate with a new AP without repeating the full authentication process.

103. According to one type of preferred embodiment in Lee, "an AP, which an STA associates with, transmits proactive keys needed for roaming to neighbor APs of the AP. When the STA moves to one of the neighbor APs, a reassociation is carried out between the STA and the neighbor AP using the already provided proactive key." Lee at Abstract. *See also* Lee at [0036]-[0039]. Lee's Fig. 7 illustrates a proactive key generation procedure in this first preferred embodiment.

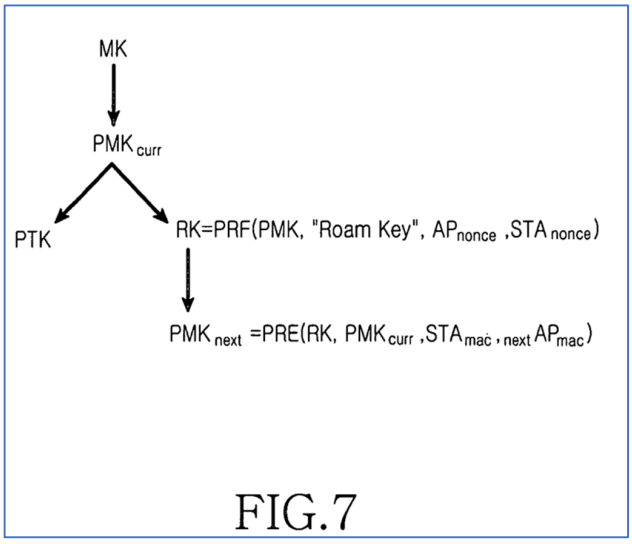


FIG.7

104. In Fig. 7, an Authentication, Authorization, and Accounting Server (AAA server), which is separate from the AP or STA, generated the PMK_{curr} from a Master Key (MK). PMK_{curr} is utilized in the authentication between the STA and the AP that it currently connects to (AP_{curr}). AP_{curr} derives a Pairwise Transient Key (PTK) and a Roam Key (RK) from PMK_{curr}. Then, PMK_{next} can be calculated with the RK derived from PMK_{curr}, PMK_{curr}, the MAC address of STA, and the MAC address of the next AP. Lee at [0086]-[0089]. For example, AP_A has two neighbors

AP_B and AP_E, AP_A would then generate a $PMK(AP_B)_{next}$ and a $PMK(AP_E)_{next}$. Lee at [0091-0094].

105. According to another type of preferred embodiment in Lee, "an authentication server transmits proactive keys needed for roaming to neighbor APs to which the STA is likely to move, so that when the STA moves to one of the neighbor APs, a reassociation is carried out between the STA and the neighbor AP using the already provided proactive key." Lee at Abstract. In this embodiment, a higher-layer server (an Accounting Server, AS) manages an AP-neighborhood graph for each AP, and is in charge of notifying neighboring APs that the STA may roam to them. According to Fig. 13 of Lee, an initial association procedure is carried out among the STA, the first AP (which the STA currently connects to) and the AS. Specifically, by receiving the Notify-Request messages from AS, the first and second neighbor APs consider that the STA may move from the first AP to them. The first neighbor AP and the second neighbor AP transmit to the AS an Access-Request message including Acct-Session-ID, Acct-Multi-Session-ID and PMK-Generation in steps 1313 and 1317, respectively, to acquire PMKs before the STA

roams. Lee at [0118]-[0121].

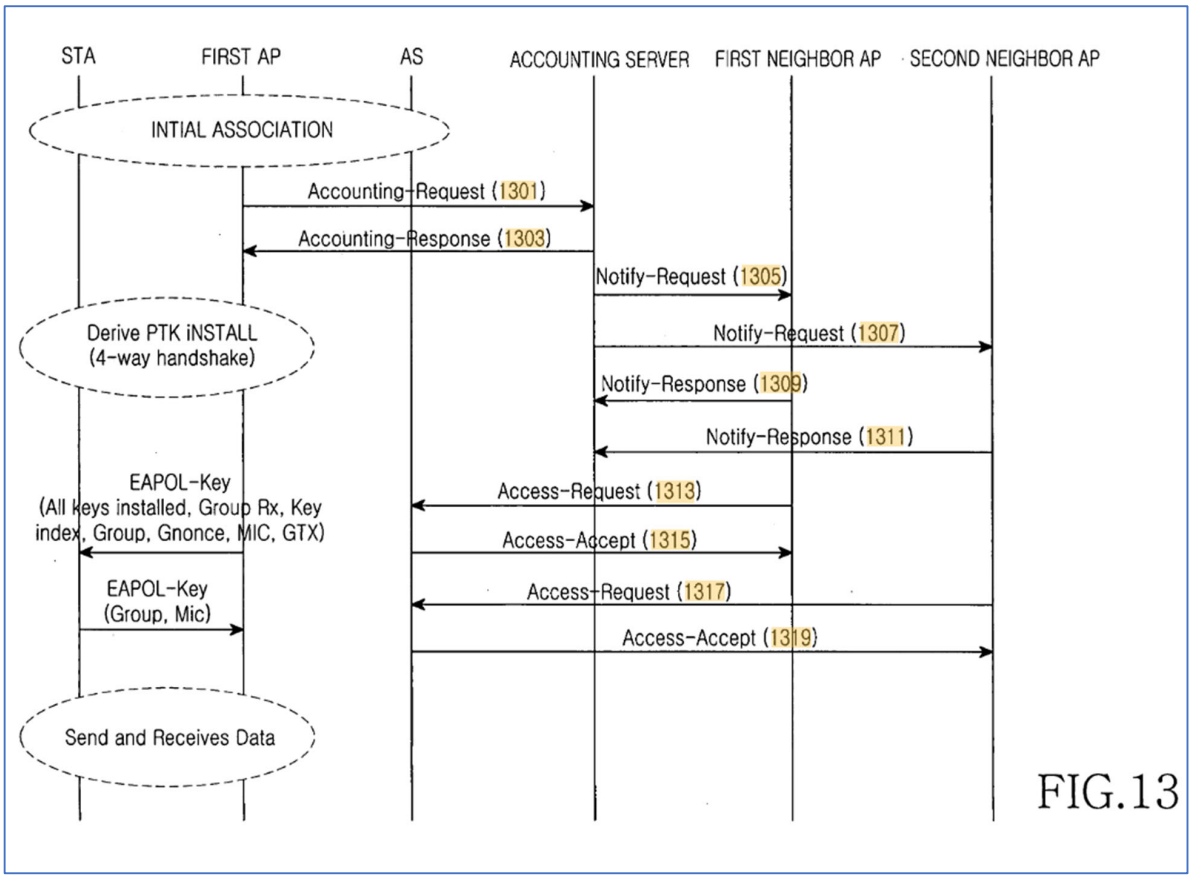


FIG.13

VIII. DR. MANDAYAM FAILS TO SHOW THE CLAIMS OF THE '671 PATENT ARE OBVIOUS IN LIGHT OF THE ALLEGED PRIOR ART

A. Ground 1 Fails to Show Claims 1-4, 7, 8, 12, 14, and 16 of the '671 Patent are Obvious Over Sood

106. It is my opinion that Dr. Mandayam has failed to show that Sood alone renders obvious any of the claims of the '671 Patent (i.e., Ground 1). My reasoning for this is provided below.

a. Claim 1

i. 1[a]: "cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods;"

107. Dr. Mandayam alleges that Sood alone teaches Claim 1[a] of the '671 Patent. He begins his analysis by explaining how "Sood discloses a key derivation in figure 7 that cryptographically binds at least R0KH-ID, R1KH-ID, and BSSID ("access network parameters") to the PTK ("a key")." Mandayam Report at ¶ 86. He also further explains with respect to Sood that "R0KH-ID, R1KH-ID, and BSSID are inputs to the KDF-PTKLen function and, thus, are bound to the PTK by the key derivation." Mandayam Report at ¶ 87. Further, Dr. Mandayam points to the '671 Patent and how it discloses "the identity of the EAP authenticator" as an example of an access network parameter. Mandayam Report at ¶ 88. Under these considerations, Dr. Mandayam then opines that Sood discloses that at least R0KH-ID and R1KH-ID[1] are advertised by the access point to the subscriber station in a "beacon". Mandayam Report at ¶ 90. However, I disagree with Dr. Mandayam's analysis; he ignores that the identity of the EAP authenticator ("AA")—which is an access

[1] I refer to R0KH-ID and R1KH-ID together as NAS-ID in my report. This is because these values are used to identify the NAS.

network parameter that is carried in an authentication method while not cryptographically bound to a key—is exchanged in the 4-way handshake described by the 802.11i standard (EX1009), which is relied upon by Sood's disclosures.

108. Although Sood advertises certain parameters via a pre-authentication beacon, Sood carries other access network parameters that are not cryptographically bound to any key—namely, the "AA" MAC Address of the Authenticator (i.e., the identity of the EAP authenticator)—during the 802.11i "four-way handshake" authentication method.

109. Sood's described embodiments use the 802.11 WLAN standard. Sood mentions "802.11" or "WLAN" at numerous points throughout its disclosures. Sood's Figures 2 and 4 also illustrate traditional 802.11 WLAN networks with AP access points and STA stations. Sood. at Figs. 2, 4. Moreover, the particular network parameters in Sood that Dr. Mandayam describes in his analysis (e.g., R0KH-ID, R1KH-ID, and BSS-ID) are specific to the 802.11 WLAN standards (both 802.11i and 802.11r). (https://standards.ieee.org/ieee/802.11r/3954/).

110. I also note that, while Sood does mention that its disclosures can be applied to other wireless networks (Sood at 2:65-3:7), Sood does not provide any technical details regarding how this would be done. In addition, Sood's disclosures also have technical incompatibilities with the networks it mentions.

111. Sood relies on the EAP protocol framework for key derivation and establishing a secure communication channel, specifically what can be referred to as "traditional EAP," which is defined in RFC 3748. While the EAP framework is used in cellular communications (3G, 4G, and 5G networks), there are fundamental differences in what is used in the cellular network standards and what is used in 802.11 networks. Because of such, Sood is limited in its application, specifically to 802.11 networks.

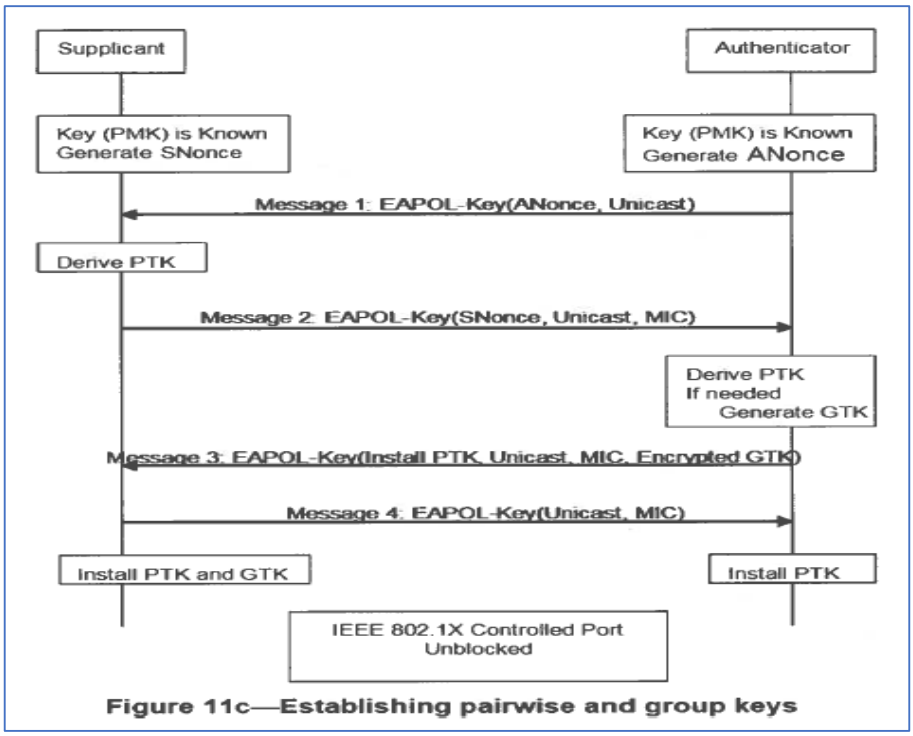
112. The EAP protocol used by UMTS(3G), LTE(4G), and NR(5G) is called EAP-AKA[2] and is a modified and more specific version of the traditional EAP protocol used in 802.11. In this variant, it relies on a shared secret that is stored on the SIM card by the telecommunications providers. That secret on the SIM is what is used as the master key in this version of EAP. This is a hard requirement by the 3GPP standards and would thus be incompatible with Sood's disclosures. Thus, there is no need to perform the same key derivation, as keys are already pre-established on the SIM cards by telecommunication providers.

113. Further, the EAP-AKA protocol was eventually revised as EAP-AKA'[3], which is an advanced version of the protocol. The standard for EAP-AKA' defines how channel binding is done and standardizes it. Thus, this further eliminates

[2] https://datatracker.ietf.org/doc/html/rfc4187
[3] https://www.rfc-editor.org/rfc/rfc5448

the applicability of Sood to mobile networks, as its disclosures expressly teach away from what is defined in the 3GPP standards. Since key management and channel binding are already standardized, cellular communication networks could not apply Sood's teachings without being incompatible with the 3GPP standards. Thus, Sood is limited in its application to 802.11 networks.

114. The 802.11 WLAN standard, specifically 802.11i, teaches that access network parameters are exchanged during the authentication method colloquially known as the "four-way handshake." 802.11i Figure 11(c) illustrates the four-way handshake, which includes four messages labeled "Message 1" to "Message 4":



EX1009 (IEEE802.11i) at 31.

115. The standard explains with respect to the diagram that, "[u]pon successful completion of the 4-Way Handshake, the Authenticator and Supplicant have authenticated each other." EX1009 (IEEE802.11i) at 31. Thus, the 802.11i Four-Way handshake is part of an authentication method.

116. Specifically, Message 1 of the four-way handshake "identifies AA as the peer STA to the Supplicant's STA." EX1009 (IEEE802.11i) at 107. The standard defines "AA" as "the IEEE 802.11X Authenticator [] MAC address." *Id*. at 18. When sent as part of Message 1, that "AA" authenticator address is not cryptographically bound to a key and sent in plaintext, as it is required for deriving the PTK Pairwise Transient Key by the supplicant. The PTK derivation by the supplicant occurs after the supplicant receives Message 1 (*Id*. at 107). This derivation is described in the following formula:

The PTK derivation step

PTK ← PRF-X(PMK, "Pairwise key expansion" || Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))

EX1009 (IEEE802.11i) at 106 (highlighting added).

117. Further, the exchange of AA in Message 1 of the 802.11i four-way handshake is supported by various resources, including protocol analyses[4], guides[5],

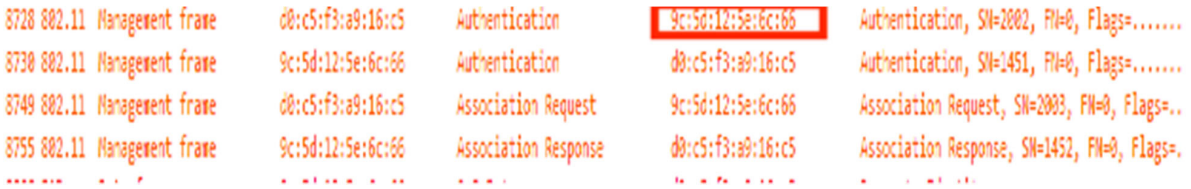
[4] https://www.wifi-professionals.com/2019/01/4-way-handshake

[5] https://networklessons.com/wireless/wpa-and-wpa2-4-way-handshake

and informational articles. [6] For example, the guide provided by "networklessons.com" explains the four-way handshake in great detail and what is performed at each step. In its description for message 1, it explains that "The client receives message one and derives the Pairwise Transient Key (PTK)". (https://networklessons.com/wireless/wpa-and-wpa2-4-way-handshake). Under that, it further explains that the client already had the PMK, S-nonce, and client MAC address values, but received the A-nonce and AP MAC address (AA) in message one. Other articles on WPA/WPA2 corroborate this as well, including explaining that "The AP also includes its MAC address and other key negotiation parameters" when describing the details of Message 1. (https://www.linkedin.com/pulse/understanding-wpa2-4-way-handshake-kola-sainikhil-pguuc)

118. This is also further reflected in publicly available protocol analyses that show that the AA is included in the message, an image from which is provided here:

[6] https://www.linkedin.com/pulse/understanding-wpa2-4-way-handshake-kola-sainikhil-pguuc



Wireshark View of Four-Way Handshake (Annotated) (https://www.wifi-professionals.com/2019/01/4-way-handshake)

119. The image shows that the MAC address of the AP (AA) (boxed in red) is sent to the supplicant in message 1. This is further explained in the descriptions of the protocol analysis that explains "Mac address 9c:5d:12:5e:6c:66 is source address or mac address of the access point who is sending first EAPOL message to the device", as well as describes message 1 as "access point sends EAPOL message with Anonce (random number) to the device to generate PTK. Don't forget client device knows AP's MAC because it's connected to it. It has PMK, Snonce and its own MAC address. Once it receives Anonce from access point, it has all the inputs to create the PTK." (https://www.wifi-professionals.com/2019/01/4-way-handshake).

120. As such, a POSITA would have understood that the AA is carried in plaintext during the four-way handshake for use in PTK derivation.

121. Thus, AA is an access network parameter that is carried, unbound to any key, as part of the four-way handshake authentication method. This disclosure of Sood contradicts the '671 independent claims, which recite "cryptographically

bind[ing] access network parameters to a [] key [] without [] needing to carry [the] parameters in [] authentication methods."

122. Even further, I also note that the 802.11i standard already mandates carriage of the RSN information element in Messages 2 and 3 of the Four-Way Handshake (§8.5.3.2, Notes 1–2). If the element is absent or altered, the STA "shall de-authenticate the peer." Consequently, a designer in 2005 who sought Wi-Fi Alliance WPA2 certification (Test Plan v1.1, 2004) would never omit these parameters; doing so would fail interoperability testing and block market entry. Lee's 2005 channel-binding proposal operates one layer higher, inside EAP-TLV, and does not modify the MAC-layer handshake introduced by 802.11i. Moreover, the identifiers Dr. Mandayam relies on (R0KH-ID, R1KH-ID) were still under debate in draft-802.11r ballots (IEEE 802.11-05/1136r0, Nov 2005) and were not part of any ratified pre-2006 text. Because a POSITA had to support the 802.11i handshake verbatim to ship products, there was no realistic motivation to strip out these parameters merely because Lee offered an alternative verification path. The Sood–Lee combination, therefore, still fails to teach—let alone render obvious—the limitation "without needing to carry the parameters in authentication methods."

123. As such, it is my opinion that Dr. Mandayam has failed to show that Sood alone discloses Claim 1[a] of the '671 Patent.

ii. 1[b]: "further including deriving a channel binding key from a channel binding master key bound to a key binding blob using a key derivation function; and"

124. Dr. Mandayam opines that Sood alone teaches Claim 1[b] of the '671 Patent. He proposes three different mappings. Mandayam Report at ¶ 94. But none of those three mappings satisfy the claim language.

125. First, it is my understanding that the parties agree that this claim language means: "[deriving a / derive said] channel binding key from a channel binding master key and binding the channel binding key to a key binding blob using a key derivation function."

126. The '671 Patent teaches that, in a preferred embodiment, "the [channel binding key] CBK is derived from a [channel binding master key] CBMK and bound to a [key binding blob] KBB associated with the authenticator using a [key derivation function] KDF." '671 Patent at 13:66-14:2. The '671 Patent further explains that, in a preferred embodiment, "a [channel binding key] CBK can be computed using [a] pseudo random function (prf+) defined in IKEv2 [RFC4306] in the following way: CBK=kdf+(CBMK, KBB); wherein KDF = Key Derivation Function." *Id*. at 14:59-64. And the highlighted portions of Figure 3 illustrate a preferred embodiment where both the KBB and the CBM are input into a single KDF, and the CBK is the output of the KDF:

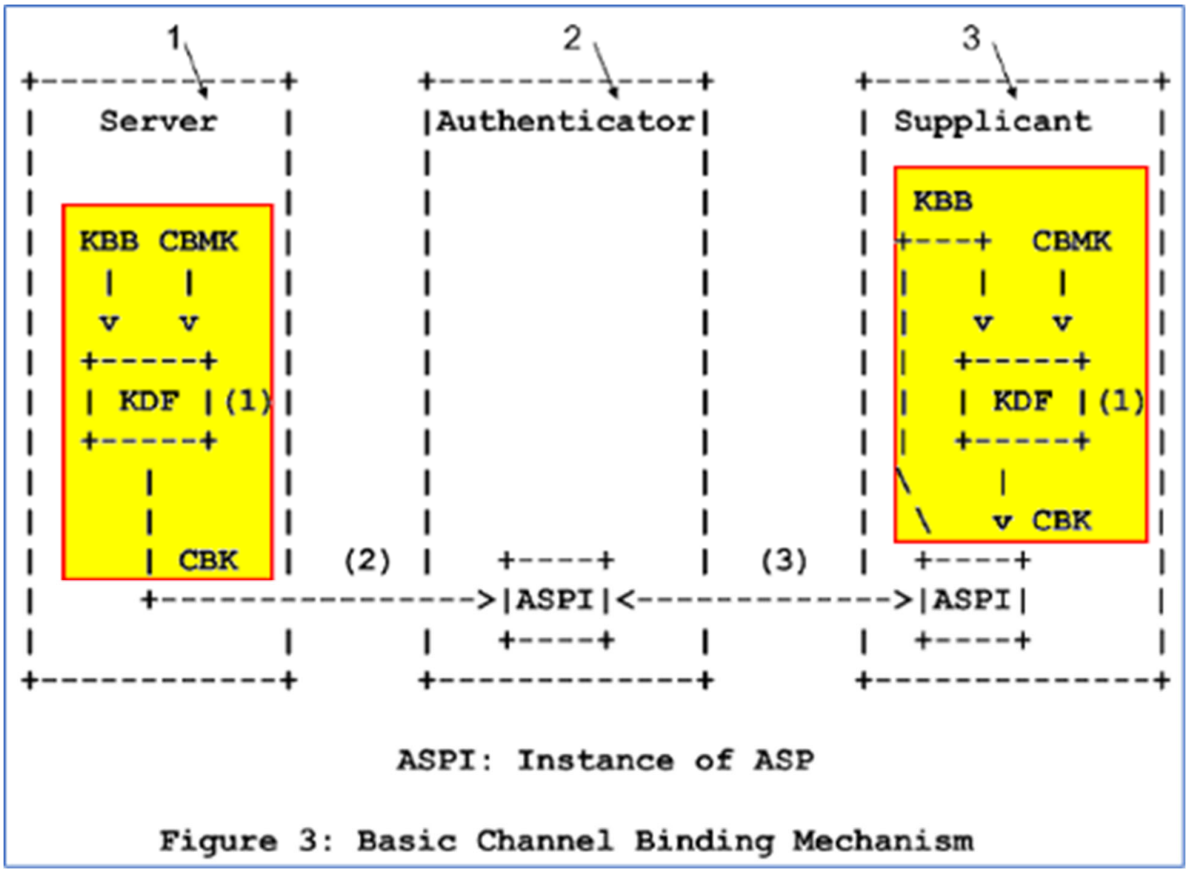


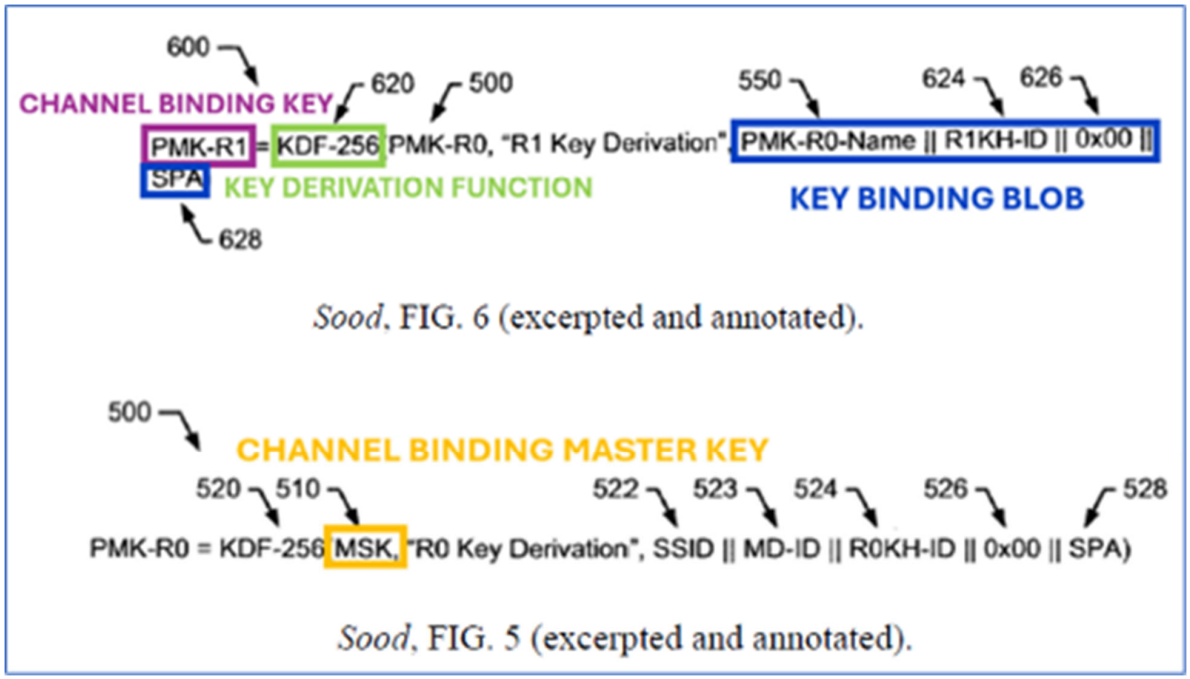
Figure 3: Basic Channel Binding Mechanism

’671 Patent Figure 3

127. Dr. Mandayam’s report relies solely on Sood to teach this claim element; for claim elements in which he describes a combination of prior art, only Sood is referenced for this particular claim element. Specifically, the report maps Sood to the claim language in three alternative ways—none of which pass muster. As explained below, none of those three mappings show one instance of Sood’s KDF-256 “key derivation function” binding Sood’s MSK “channel binding master key” to Sood’s “channel binding key.”

1. Dr. Mandayam's First Mapping Fails

128. For this mapping, Dr. Mandayam refers to Sood's disclosures for deriving the keys PMK-R0 and PMK-R1, which are depicted in Figures 5 and 6 of Sood. Mandayam Report at ¶¶s 95-96. Dr. Mandayam's annotated figures are provided here:



Mandayam Report at ¶ 95

129. What Dr. Mandayam claims is the "channel binding master key" is Sood's master secret key 510 (MSK), shown in Figure 5. He also claims that the "channel binding key" is Sood's second-level derived authentication key 600 (PMK-R1), shown in Figure 6. Moreover, this mapping by Dr. Mandayam claims the "key binding blob" is Sood's concatenation of (i) the name of the first-level derived authentication key 550 (PMK-R0-Name) with (ii) the NAS identifier field 624

containing the IP address of the network entity holding the second-level derived authentication key (R1KH-ID), (iii) the separator field 626 used to prevent sliding window or perimeter attacks (0x00), and (iv) the sender protocol address 628 containing the MAC address of the subscriber station (SPA). This is reflected in his annotated Figure 6 shown above. Finally, this mapping also assumes the claimed "key derivation function" is a particular instance of the 256-bit key derivation function 620 (KDF-256). This is also shown in Dr. Mandayam's annotated Figure 6 shown above.

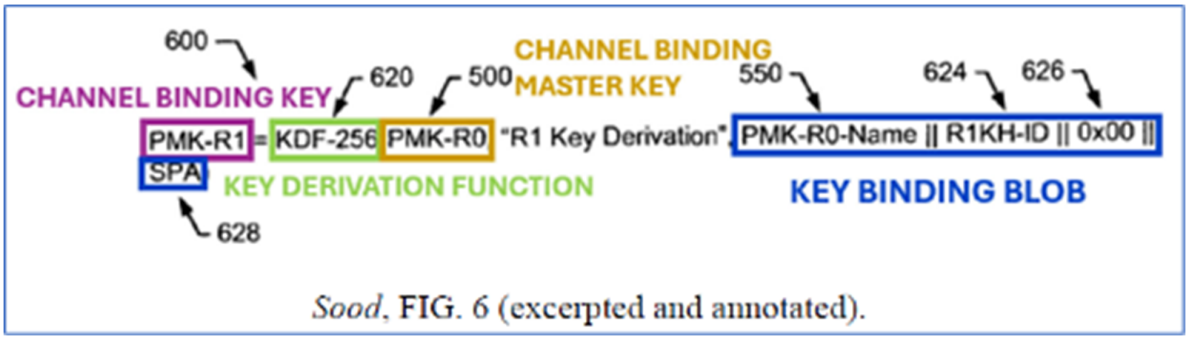
130. However, this first mapping by Mandayam does not satisfy the claim language. The alleged key derivation function (in green) is not used to derive the alleged channel binding key (in purple) from the alleged channel binding master key (in yellow), as claimed. Rather, Sood Figure 6 shows, at most, the alleged key derivation function (in green) being used to derive the alleged channel binding key (in purple) from a first-level derived authentication key 550, PMK-R0. But Sood does not teach that first-level derived authentication key 550 is the claimed "channel binding master key." Rather, Sood teaches that its "channel binding master key" is master secret key/master authentication key MSK 510. Sood at 6:51-56; *see also* '671 at 13:25. Sood's MSK 510 is generated when the authentication server 210 and the subscriber station communicate with each other as part of the authentication step 410. Sood at 6:51-56. And this MSK 510 may be used to generate a first-level

derived authentication key (e.g., PMK-R0), as shown in Figure 5. *Id*. at 6:56-66. But Sood Figure 6 does not teach or suggest using the alleged key derivation function (in green) to derive the alleged channel binding key (in purple) from MSK 510 (what Sood teaches is its channel binding "master" key); MSK 510 is not part of the Figure 6 equation.

131. Therefore, Dr. Mandayam's first proposed mapping does not meet the language of Claim 1[b].

2. Dr. Mandayam's Second Mapping Fails

132. For this second mapping, Dr. Mandayam refers to Sood's disclosures for deriving the key PMK-R1, which are depicted in Figure 6 of Sood. Mandayam Report at ¶ 97. Dr. Mandayam's annotated figures are provided here:



Sood, FIG. 6 (excerpted and annotated).

(Exhibit 1002 ¶97*)*

133. In this mapping, Dr. Mandayam alleges that PMK-R0 (Sood's first-level derived authentication key) is the "channel binding master key" required by the claim language. He opines in this mapping that PMK-R1 (Sood's second-level derived authentication key) is the "channel binding key" and the claimed "key

binding blob" is Sood's concatenation of (i) the name of the first-level derived authentication key 550 (PMK-R0-Name) with (ii) the NAS identifier field 624 containing the IP address of the network entity holding the second-level derived authentication key (R1KH-ID), (iii) the separator field 626 used to prevent sliding window or perimeter attacks (0x00), and (iv) the sender protocol address 628 containing the MAC address of the subscriber station (SPA). Additionally, Dr. Mandayam's mapping also alleges that the claimed "key derivation function" is a particular instance of the 256-bit key derivation function 620 (KDF-256). All of Dr. Mandayam's proposed mapping is shown in his annotated Figure 6 of Sood provided above.

134. However, Dr. Mandayam's second mapping does not satisfy the claim language, either. As discussed above, Sood does not teach that the first-level derived authentication key 500 (PMK-R0) is the claimed "channel binding master key." Rather, Sood teaches that its "channel binding master key" is the master secret key/master authentication key MSK 510. Sood at 6:51-56; *see also* '671 at 13:25 ("an MSK [] is a CBMK). Sood's MSK 510 is generated when the authentication server 210 and the subscriber station communicate with each other as part of the authentication step 410. Sood at 6:51-56. And this MSK 510 may be used to generate a first-level derived authentication key (e.g., PMK-R0), as shown in Figure 5. *Id*. at 6:56-66. But MSK 510 is not part of the Figure 6 equation that is central to Dr.

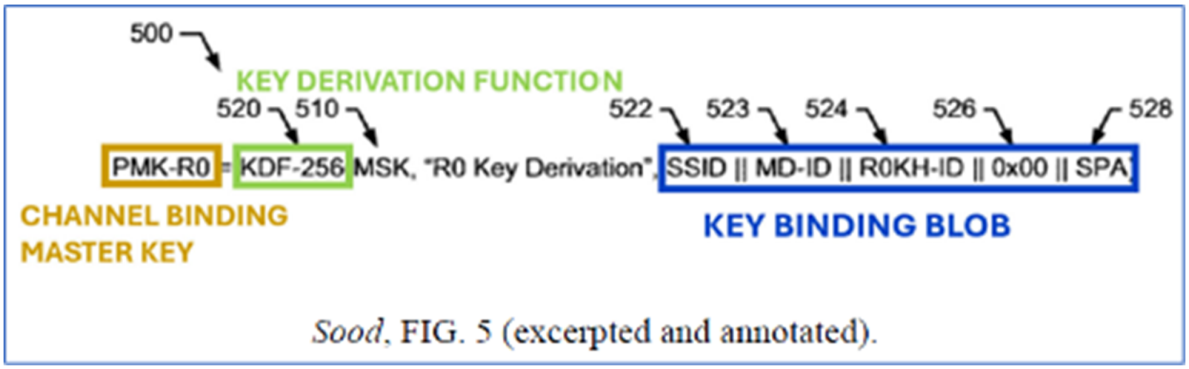
Mandayam's second mapping. Accordingly, Dr. Mandayam's second mapping from Fig. 6 does not show deriving a channel binding key from a "channel binding master key," as required by the claims.

135. Therefore, Dr. Mandayam's second proposed mapping does not meet the language of Claim 1[b], either

3. Dr. Mandayam's Third Mapping Fails

136. Though Dr. Mandayam originally indicates he only proposes 2 mappings, he also suggests a third later in his analysis for Claim 1[b], which I also address. Mandayam Report at ¶¶222-234.

137. In Dr. Mandayam's third mapping, he does not even allege there is a "channel binding key". Instead, he only alleges that the claimed "channel binding master key" is Sood's first-level derived authentication key 500 (PMK-R0) and that the claimed "key binding blob" is Sood's concatenation of (i) the service set identifier field 522 (SSID) with (ii) the mobility domain identifier field 523 (MD-ID), (iii) the NAS identifier field 524 containing the IP address of the network entity holding the first-level derived authentication key (R0KH-ID), (iv) the separator field 526 used to prevent sliding window or perimeter attacks (0x00), and (iv) the sender protocol address 528 containing the MAC address of the subscriber station (SPA). Dr. Mandayam's third mapping relies on his annotated Figure 5 of Sood, which is provided here:



Sood, FIG. 5 (excerpted and annotated).

Mandayam Report at ¶ 112

138. This third mapping also does not satisfy the claim language for at least two reasons. First, it is based on an erroneous claim construction. For this third mapping, Dr. Mandayam references the disclosure in Sood "that PMK-R0 ("channel binding master key") is bound to the concatenation of SSID, MD-ID, R0KH-ID, 0x00, and SPA ("key binding blob") using the function KDF-256." Mandayam Report at ¶ 112. However, it is my understanding that the Parties and Dr. Mandayam agree that the claim language requires the key binding blob to be bound to the channel binding key. Accordingly, this third mapping fails because it does not apply the agreed claim construction. Second, Dr. Mandayam's mapping does not include a "channel binding key" as required by the claim language. Mandayam Report at ¶¶s 112-115. As such, Dr. Mandayam's third mapping fails because it does not satisfy all the claim elements, including explaining how Sood derives a channel binding key.

139. Thus, Dr. Mandayam's proposed third mapping does not meet the language of Claim 1[b].

140. Therefore, it is my opinion that Dr. Mandayam has failed to show Sood alone discloses Claim 1[b] of the '671 Patent with any of his three proposed mappings.

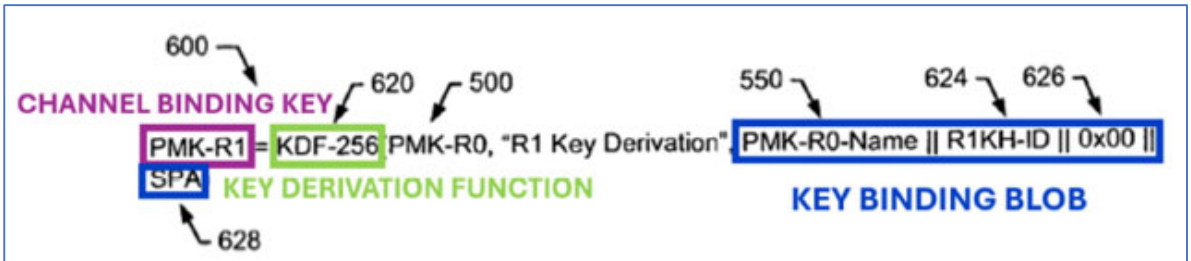
iii. 1[c]: "wherein said key binding blob is a string that is constructed from static parameters advertised from an authenticator."

141. In his analysis for Claim 1[c], Dr. Mandayam simply cites back to his analysis for Claim 1[b], as he alleges it explains how Sood teaches a "channel binding blob". He does not provide any new analysis or evidence. Thus, I incorporate my analysis from Claim 1[b] by reference.

142. Additionally, I elaborate my analysis from Claim 1[b] and Dr. Mandayam's discussion regarding the "key binding blob".

143. Dr. Mandayam maps the claimed "key binding blob" to Sood's concatenation of four parameters: (1) the name of the first-level derived authentication key 550 (PMK-R0-Name) with (2) the NAS identifier field 624 containing the IP address of the network entity holding the second-level derived authentication key (R1KH-ID), (3) the separator field 626 used to prevent sliding window or perimeter attacks (0x00), and (4) the sender protocol address 628

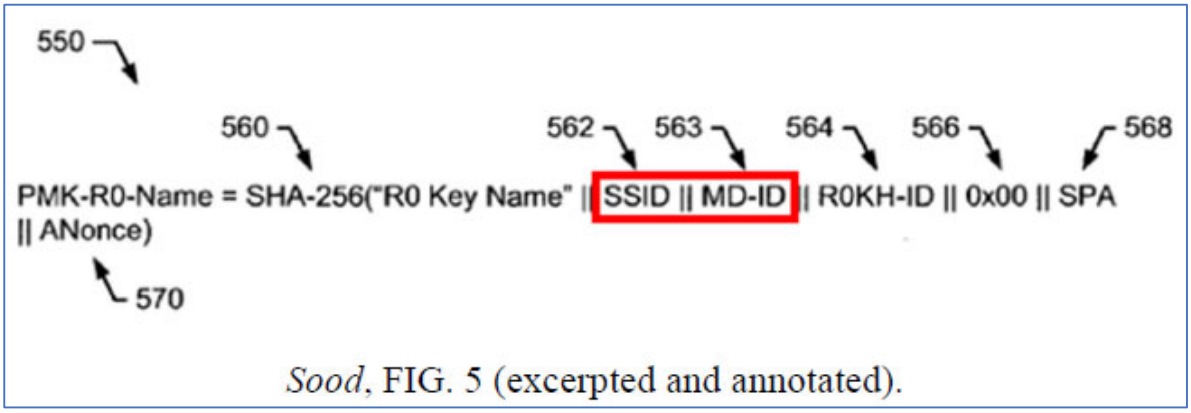
containing the MAC address of the subscriber station (SPA). This is explained in his third mapping and is shown in his annotated version of Sood's Figure 6:



Sood, FIG. 6 (excerpted and annotated).

Mandayam Report at ¶ 95

144. However, Dr. Mandayam only explains why two of those four parameters are "static parameters advertised from [an] authenticator," as required by the '671 claims. Dr. Mandayam explains that R1KH-ID is static because it is an identifier of a "network entity," citing Sood at 8:27-30. Mandayam Report at ¶ 106. Dr. Mandayam also explains that PMK-R0-Name is static as it is constructed using SSID and MD-ID, each of which is allegedly static and advertised from an authenticator. Mandayam Report at ¶ 109. He then provides the following annotated image from Sood to support his claim:



Sood, FIG. 5 (excerpted and annotated).

Mandayam Report at ¶ 109.

145. Despite his evidence for the first two parameters, Dr. Mandayam does not address why the third and fourth parameters in Sood's alleged "key binding blob", which includes (3) "0x00", the separator field used to prevent sliding window or perimeter attacks and (4) "SPA" 628, the sender protocol address containing the MAC address of the subscriber station, are "static parameters advertised from [an] authenticator". Additionally, Sood's teachings would suggest otherwise.

146. Sood teaches that the third parameter, separator field, includes "a value added after variable length fields to prevent sliding window or parameter attacks on the KDF." Sood at 8:37-39. For example, "the separator field 626 may include a value within a range from 0x00 to 0x7F." *Id*. at 8:39-41. Sood also does not disclose where this separator value originates from.

147. It is, thus, my opinion that Dr. Mandayam has failed to show that Sood alone discloses Claim 1[c] of the '671 Patent.

148. As a result, it is also my opinion that, because of Dr. Mandayam's failure to show Sood discloses all the elements of Claim 1 of the '671 Patent, he has not shown that Sood alone renders obvious Claim 1 of the '671 Patent.

b. Claim 2: "The method of claim 1, wherein said authentication methods include EAP methods."

149. Claim 2 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claim 2 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 2 is rendered obvious by the alleged prior art for at least this reason.

c. Claim 3: "The method of claim 1, wherein said parameters include parameters advertised by an authenticator to said supplicant."

150. Claim 3 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claim 3 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 3 is rendered obvious by the alleged prior art for at least this reason.

d. Claim 4: "The method of claim 3, wherein the identity of the authenticator is one of said parameters."

151. Claim 4 of the '671 Patent is dependent on Claim 3. As I have previously discussed in my analysis for Claim 3, Dr. Mandayam has failed to show that Claim 3 is rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claim 4 is dependent on Claim 3, Dr. Mandayam has also failed to show Claim 4 is rendered obvious by the alleged prior art for at least this reason.

e. Claim 7: "The method of claim 1, wherein said key binding blob is an octet-string that is constructed from static parameters advertised from an authenticator using an authenticator-supplicant protocol."

152. Claim 7 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claim 7 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 7 is rendered obvious by the alleged prior art for at least this reason.

f. Claim 8: "The method of claim 1, including a network side authenticator and said supplicant using the channel binding

master key for protecting an authenticator-supplicant protocol."

153. Claim 8 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claim 8 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 8 is rendered obvious by the alleged prior art for at least this reason.

g. Claim 12: "The method of claim 1, further including creating multiple channel binding keys from a single channel binding master key for multiple authenticators."

154. Claim 12 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claim 12 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 12 is rendered obvious by the alleged prior art for at least this reason.

h. Claims 14, 16: "The method of claim [1/12], further including creating multiple channel binding keys from a single channel

binding master key for multiple authenticators using different key binding blobs for different authenticators."

155. Claims 14 and 16 of the '671 Patent are dependent on Claims 1 and 12, respectively. As I have previously discussed in my analyses for Claims 1 and 12, Dr. Mandayam has failed to show that Claims 1 and 12 are rendered obvious in light of Sood alone. Therefore, it is also my opinion that because Claims 14 and 16 are dependent on Claims 1 and 12, respectively, Dr. Mandayam has also failed to show Claims 14 and 16 are rendered obvious by the alleged prior art for at least this reason.

B. Ground 2 Fails to Show Claims 5 and 18 of the '671 Patent are Obvious Over the Combination of Sood and Aboba

156. It is my opinion that Dr. Mandayam has failed to show that Sood in combination with Aboba renders obvious any of the claims of the '671 Patent (i.e., Ground 2). My reasoning for this is provided below.

a. Claim 5: "The method of claim 1, wherein said channel binding master key is at least 64 octets long."

157. Claim 5 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Dr. Mandayam has also not shown that the combination with Aboba remedies the deficiencies of his analysis for Claim 1. Therefore, it is also my opinion that because Claim 5 is dependent on Claim

1, Dr. Mandayam has also failed to show Claim 5 is rendered obvious by the alleged prior art for at least this reason.

b. Claim 18: "The method of claim 1, wherein said key derivation function is computed based on CBK=kdf+(CBMK, KBB), where CBK represents channel binding key, CBMK represents channel binding master key, and KBB represents key binding blob."

158. Claim 18 of the '671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Dr. Mandayam has also not shown that the combination with Aboba remedies the deficiencies of his analysis for Claim 1. Therefore, it is also my opinion that because Claim 18 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 18 is rendered obvious by the alleged prior art for at least this reason.

C. Ground 3 Fails to Show Claims 6, 10, 11, 13, 15, 17, and 19 of the '671 Patent are Obvious Over the Combination of Sood and Lee

159. It is my opinion that Dr. Mandayam has failed to show that Sood in combination with Lee renders obvious any of the claims of the '671 Patent (i.e., Ground 3). My reasoning for this is provided below.

a. Claim 6

i. 6[a]: "using an extensible authentication protocol server to cryptographically bind access network parameters to a channel binding key and to transmit said channel binding key to an extensible authentication protocol authenticator for use by the extensible authentication protocol authenticator as an extensible authentication protocol master session key without said extensible authentication protocol authenticator needing to carry said access network parameters in extensible authentication protocol authentication methods;"

160. Dr. Mandayam's arguments for Claim 6[a] rely on his analyses for Claim 1[a] and 1[b]. He simply cites back to his analyses for Claim 1[a] and 6[b], while making minor additions to adapt to the specific language of Claim 6[a]. As such, Dr. Mandayam's arguments for Claim 6[a] are deficient for the same reasoning I described in my analyses for Claim 1[a], 1[b], and 1[c]. I incorporate each of those sections here by reference.

161. Thus, my opinion that Dr. Mandayam has failed to show that Sood in combination with Lee discloses Claim 6[a] of the '671 Patent.

ii. 6[b]: "including using said extensible authentication protocol server to derive said channel binding key from a channel binding master key bound to a key binding blob using a key derivation function;"

162. Dr. Mandayam does not present any new arguments for Claim 6[b]. He simply cites back to his analyses for Claim 1[b]. As such, Dr. Mandayam's arguments for Claim 6[b] are deficient for the same reasoning I described in my analyses for Claim 1[b] and 1[c]. I incorporate each of those sections here by reference.

163. As such, it is my opinion that Dr. Mandayam has failed to show that Sood in combination with Lee discloses Claim 6[b] of the '671 Patent.

iii. 6[c]: "wherein said key binding blob is a string that is constructed from static parameters advertised from said extensible authentication protocol authenticator."

164. Dr. Mandayam does not present any new arguments for Claim 6[c]. He simply cites back to his analyses for Claim 1[b] and 6[a]. As such, Dr. Mandayam's arguments for Claim 6[c] are deficient for the same reasoning I described in my analyses for Claim 1[b], 1[c], and 6[a]. I incorporate each of those sections here by reference.

165. It is, thus, my opinion that Dr. Mandayam has failed to show that Sood in combination with Lee discloses Claim 6[c] of the ’671 Patent.

166. As a result, it is also my opinion that because of Dr. Mandayam’s failure to show Sood in combination with Lee discloses all the elements of Claim 6 of the ’671 Patent, he has not shown that Sood in combination with Lee renders obvious Claim 6 of the ’671 Patent.

b. Claim 10: “The method of claim 1, further including that: a) a server and the supplicant create a channel binding key used for an authenticator; b) the server transfers the channel binding key to the authenticator; and c) the supplicant and the authenticator verify proof of possession of the channel binding key over an authenticator-supplicant protocol.”

167. Claim 10 of the ’671 Patent is dependent on Claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Dr. Mandayam has also not shown that the combination with Lee remedies the deficiencies of his analysis for Claim 1. Therefore, it is also my opinion that because Claim 10 is dependent on Claim 1, Dr. Mandayam has also failed to show Claim 10 is rendered obvious by the alleged prior art for at least this reason.

c. Claim 11: "The method of claim 10, further including that the channel binding key is derived from a channel binding master key bound to a key binding blob associated with the authenticator using a key derivation function."

168. Claim 11 of the '671 Patent is dependent on Claim 10. As I have previously discussed in my analysis for Claim 10, Dr. Mandayam has failed to show that Claim 10 is rendered obvious in light of Sood in combination with Lee. Therefore, it is also my opinion that because Claim 11 is dependent on Claim 10, Dr. Mandayam has also failed to show Claim 11 is rendered obvious by the alleged prior art for at least this reason.

d. Claims 13, 15, 17: "The method of claim [12/14/16], further including using channel binding keys to form a hierarchical channel binding."

169. Claims 13, 15, and 17 of the '671 Patent are dependent on Claims 12, 14, and 16, respectively. As I have previously discussed in my analyses for Claims 12, 14, and 16, Dr. Mandayam has failed to show that any of these claims are rendered obvious in light of Sood alone. Dr. Mandayam has also not shown that the combination with Lee remedies the deficiencies of his analyses for Claims 12, 14, and 16. Therefore, it is also my opinion that because Claims 13, 15, and 17 are dependent on Claims 12, 14, and 16, respectively, Dr. Mandayam has also failed to

show Claims 13, 15, and 17 are rendered obvious by the alleged prior art for at least this reason.

e. Claim 19: "The method of claim 3, wherein said authenticator is an EAP authenticator, and wherein the EAP authenticator receives and processes the channel binding key as a Master Session Key (MSK)."

170. Claim 19 of the '671 Patent is dependent on Claim 3, which is dependent on claim 1. As I have previously discussed in my analysis for Claim 1, Dr. Mandayam has failed to show that Claim 1 is rendered obvious in light of Sood alone. Dr. Mandayam has also not shown that the combination with Lee remedies the deficiencies of his analysis for Claim 1. Therefore, it is also my opinion that because Claim 19 is ultimately dependent on Claim 1, Dr. Mandayam has also failed to show Claim 19 is rendered obvious by the alleged prior art for at least this reason.

D. Ground 4 Fails to Show Claims 1-8 and 10-19 of the '671 Patent are Obvious Over the Combination of Sood, Aboba, and Lee

171. It is my opinion that Dr. Mandayam has failed to show that Sood in combination with Aboba and Lee renders obvious any of the claims of the '671 Patent (i.e., Ground 4). My reasoning for this is provided below.

a. "without needing to carry the parameters in authentication methods" / "without … needing to carry said access network parameters in … authentication methods"

172. Dr. Mandayam alleges that combining Sood with Aboba and/or Lee would remedy any potential deficiencies in his arguments that Sood alone teaches the language of "without needing to carry the parameters in authentication methods" / "without … needing to carry said access network parameters in … authentication methods". Mandayam Report at ¶ 228. However, I disagree with Dr. Mandayam's analysis for the reasons provided below.

173. First, in my analysis for Claim 1[a], I explain how Sood does not disclose the same claim language Dr. Mandayam presents in this section of his report. I incorporate that analysis here by reference. As such, Dr. Mandayam's analysis presented in this section argues that Sood in combination with Lee remedies the deficiencies in his arguments for Sood alone.

174. Moreover, Dr. Mandayam argues in ground 4 that Sood can be combined with Aboba and Lee in order to cure any weaknesses in the disclosure of Sood alone (Mandayam at 222). Dr. Mandayam's arguments with respect to the combination of Sood, Aboba and Lee do not change my opinions with respect to the deficiencies in Sood, nor does Dr. Mandayam convince me that this combination renders any Claims of the '671 Patent obvious, because the concerns that I previously

voiced with respect to Sood alone also apply to the combination of Sood, Aboba and Lee.

175. For example, Dr. Mandayam argues that "all challenged claims recite 'without needing to carry the parameters in authentication methods...'" (Mandayam at 228). Dr. Mandayam contends that, "For the reasons I explained in §X.C.1 (Ground 3, Motivation to Combine Sood and Lee), these bindings would also have been performed by the server in the Sood-Lee combination." *Id.* at 231. But as I have already explained in my rebuttal to Dr. Mandayam's earlier section, these parameters must be carried in the four-way handshake in order to preserve compatibility with 802.11i. As such, I disagree that the addition of Lee here does anything to cure the previous deficiency that I have identified in this argument. A POSITA would not be motivated to ignore a required handshake in a system implementation merely because the data were sometimes available elsewhere in non-standard-compliant implementations of the system.

176. Therefore, it is my opinion that Dr. Mandaya has not remedied the deficiencies in disclosing the claim language of "without needing to carry the parameters in authentication methods" / "without … needing to carry said access network parameters in … authentication methods" through combining Sood with Aboba and/or Lee.

IX. CONCLUSION

177. I reserve the right to supplement my opinions to respond to any new arguments that the Petitioners raise. This declaration represents only those opinions that I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information that becomes available to me.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: June 23, 2025

By:

Aviel D. Rubin, Ph.D.

Appendix A

Aviel D. Rubin, Ph.D.

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

avirubin@gmail.com
https://www.linkedin.com/in/avirubin/

Overview

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

Academic Degrees

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

Academic Appointments

September, 2023 - present
Professor Emeritus, Johns Hopkins University
April, 2004 - August, 2023
Professor (with tenure), Johns Hopkins University
August, 2010 - July, 2011
Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel
January, 2003 - April, 2004
Associate Professor, Johns Hopkins University
January, 2003 - August, 2023
Technical Director, Johns Hopkins University Information Security Institute
2006 - 2010

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 78 of 101

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 Experts, Founder & Managing Partner
Harbor Labs, Founder
2005 - 2011
Independent Security Evaluators, Founder & President
1997 - 2002

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 79 of 101

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.

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 80 of 101

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

Refereed Conference Publications

- David Inyangson, Aditya Gaur, Atheer Almogbil, Tushar Jois, Aviel D. Rubin, *SoK: Security in the Inaudible World*, ACM Conference on Security and Privacy in Wireless and Mobile Networks 2025 (WiSec '25), (July, 2025).
- Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, Gabriel Kaptchuk, Aviel D. Rubin, *SocIoTy: Practical Cryptography in Smart Home Contexts,* Privacy Enhancing Technologies Symposium 2024 (PETS '24), (July, 2024).
- Atheer Almogbil , Momo Steele , Sofia Belikovetsky , Adil Inam, Olivia Wu, Aviel Rubin, Adam Bates, *Using Behavior Monitoring to Identify Privacy Concerns in Smarthome Environments,* NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec), (February, 2024).
- Samra Kasim, Nawal Valliani, Nelson Ka Ki Wong, Shahin Samadi, Lanier Watkins and Aviel Rubin, *Explainable Autonomic Cybersecurity for Industrial Control Systems*, IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), (March, 2023).

- Valeti Manoj, Shao Wenda, Niu Sihan, Christopher Rouff, Lanier Watkins, Aviel Rubin, *Cybersecurity as a Tic-Tac-Toe Game Using Autonomous Forwards (Attacking) And Backwards (Defending) Penetration Testing in a Cyber Adversarial Artificial Intelligence System*, IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM),(October, 2022).
- James Cervini & Aviel D. Rubin, *Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack*, ICCWS 17th International Conference on Cyber W arfare 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 (IoTaIS'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).

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 82 of 101

- 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).

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 83 of 101

- 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).

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 85 of 101

- Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, Financial Cryptography Conference, (February, 2000).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device,* 6th ACM Conference on Computer and Communications Security, (November, 1999).
- Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords*, 8th USENIX Security Symposium, (August, 1999).
- Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Fabian Monrose, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground,* Proc. IEEE Symposium on Security and Privacy (May, 1998).
- Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread Email in an Untrusted Network*, Second Australasian Conference on Information Security and Privacy (July, 1997).
- Fabian Monrose and Aviel D. Rubin, *Authentication via Keystroke Dynamics*, 4th ACM Conference on Computer and Communications Security (April, 1997).
- David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1997).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content,* Proc. 6th USENIX Security Symposium (July, 1996).
- Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, Proc. of Eurocrypt '96 (May, 1996).
- Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
- Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
- Aviel D. Rubin*, PseudoRandom Functions for OneTime Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
- Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).
- Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
- Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

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

Professional Activities

Board of Directors

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

Editorial and Committees

Chair: IEEE Security & Privacy Symposium Test of Time Awards Committee for 2008-2010 Conferences, May, 2020.
Associate Editor: IEEE Transactions on Information Forensics and Security (2009 - 2011).
Associate Editor: Communications of the ACM (CACM), 2009 - 2017.
Guest Co-Editor: IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, December 1, 2009.
Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting, October/November, 2007.
Associate Editor: IEEE Transactions on Software Engineering (20052006). 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 (20042006).
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 (20022005).
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 Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
- **Program Committee member:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.
- **Invited Talks Co-Coordinator**: 17th USENIX Security Symposium, San Jose, CA, July 28 August 1, 2008.
- **Program Co-chair**: (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 1822, 2008.
- Program Co-chair: (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
- **Program Committee member**: IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.

- **Program Committee member**: Financial Cryptography '04 Key West, Florida, February 9-12, 2004.
- **Program Committee member**: 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
- **Program Committee member**: 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
- **Program Committee member**: 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
- **Program Vice Chair**: Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 2024, 2003.
- **Program Committee member**: IEEE Symposium on Security and Privacy, Oakland, California, May 1114, 2003.
- **Program Committee member**: Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
- **Program Committee member**: 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRDL), Singapore December 912, 2002.
- **Program Committee member**: ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
- **Program Committee member**: 9th ACM Conference on Computer and Communications Security, Washington D.C., November 1721, 2002.
- **Program Committee member**: 5th International Conference on Electronic Commerce Research (ICECR5), Montreal, Canada, October 2327, 2002.
- **Program Committee member**: 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 1415, 2002.
- **Program Committee member**: 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 1416, 2002.
- **Program Committee member**: 11th USENIX Security Symposium, San Francisco, Ca, August 59, 2002.
- **Program Committee member**: International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 2124, 2002.
- **Program Committee member**: 11th International World Wide Web Conference Honolulu, Hawaii, May 711, 2002.
- **Program Committee member**: 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 1415, 2002.
- **Program Committee member**: The 1st International Workshop on PeertoPeer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 78, 2002.
- **Program Committee member**: The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001. Program Committee member: 10th USENIX Security Symposium, Washington D.C., August 1317, 2001.
- **Program Committee member**: Financial Cryptography '01 Grand Cayman, Cayman Islands, BWI, February, 2001.
- **Program Co-chair**: (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 79, 2001.

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

Panels

- **Panelist:** TLTF Conference: Shielding Your Business: Cybersecurity & Vendor Risk Management, Miami, Florida (December 4, 2024).
- **Panelist:** CyberTech Global Conference: The Post-COVID Cyber Challenges in the Health Sector, UAE-Dubai (April 6, 2021).
- **Panel Organizer and Moderator**: USENIX Security Conference: The 2020 Election: Remote Voting, Disinformation, and Audit (August 12, 2020).
- **Panelist:** Cardozo Society Associated panel: Cybersecurity and Privacy Law in the Digital Era, Baltimore, MD (February 19, 2020).
- **Panelist**: Washington Post panel: Hacking Health, Washington DC (June 14, 2016).
- **Panelist**: Financial Cryptography Conference, Security & Privacy, Barbados (February 24, 2016).
- **Panelist**: RSA Conference, Social Networks Security Panel, San Francisco, CA (April 21, 2015).
- **Panelist**: Expert Witness in Mock Trial: FTC Data Security, 63rd American Bar Association Section of Antitrust Law Spring Meeting Washington DC, (April 15, 2015).

- **Panelist**: Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
- **Panelist**: Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).
- **Panelist**: Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
- **Panelist**: First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
- **Panelist**: Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
- **Panelist**: Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel (May 18, 2009).
- **Panelist**: RSA Conference, Exploiting Online Games, San Francisco, CA (April 23, 2009).
- **Panelist**: American Association for the Advancement of Science, Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel, Washington DC, (November 27, 2006).
- **Panelist**: California Secretary of State's Voting System Testing Summit, Security Panel, Sacramento, CA, (November 2829, 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).

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 91 of 101

- **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 Stated 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 Stated House Committee on Science, Space, and Technology, Full Committee Hearing Is My Data on Healthcare.gov Secure?, Washington, D.C., (November 19, 2013).
- United Stated House Committee on Oversight and Government Reform, hearing on electronic voting, Washington, D.C., (April 18, 2007).
- United Stated House Committee on Appropriations, hearing on ensuring the integrity of elections, Washington, D.C., (March 7, 2007).
- Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, Hearing on Senate Bill 392 for VoterVerified Records in Voting Systems, Annapolis, MD, (February 22, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 18 for improving voting systems in Maryland, Annapolis, MD, (February 1, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland, Annapolis, MD, (February 1, 2006).
- United States Election Assistance Commission, Hearing on Voluntary Voting Systems Guidelines, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).

- Senate hearing: Voting in 2004: A Report to the Nation on America's Election Process, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
- United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, Public Hearings on Computer Security and Transparency, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).
- United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, Hearing on Electronic Voting, Washington, D.C. (July 20, 2004).
- United States House Committee on House Administration, Expert Testimony, Hearing on Security of Electronic Voting, Washington, D.C. (July 7, 2004).
- United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
- United States Election Assistance Commission, Expert Testimony, Hearing on Electronic Voting Security, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

- **Proxense, LLC**, vs. Microsoft Corporation, Case # 6:23-cv-00319-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
  - Expert Testimony at deposition, Annapolis, MD (May 13, 2025).
- **US Dominion, Inc**.. vs. Sidney Powell P.C., Case # 1:21-cv-00040-CJN-MAU, Susman Godfrey, United States District Court, District of Columbia. (Defamation)
  - Expert Testimony at deposition, Annapolis, MD (April 11, 2025).
- **US Dominion, Inc**.. vs. Herring Networks, Inc, Case # 1:21-cv-02130-CJN-MAU, Susman Godfrey, United States District Court, District of Columbia. (Defamation)
  - Expert Testimony at deposition, Annapolis, MD (April 10, 2025).
- Zoll Data Systems, Inc. vs. **Wave/Experian**, Case # 24-cv-00584-DDD-KAS, Jones Day, United States District Court, Central District of Colorado (Trade Secret)
  - Expert Testimony at Preliminary Injunction hearing, Denver, CO (February 27, 2025).
- Datavant, Inc. vs. **Vigilytics LLC**, IPR2024-00381, Fish & Richardson, US Patent Trial and Appeal Board. (Patent Validity)
  - Expert Testimony at deposition, Stuart, FL (February 17, 2025).
- **WSOU Investments, LLC**, vs. Cisco Systems Inc., Case # 6:21-cv-00128-ADA; Susman Godfrey/Folio Law Group, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
  - Expert Testimony at Trial, Waco, Texas (February 10 & 11, 2025).
  - Expert Testimony at deposition, Annapolis, MD (March 30, 2023).
  - Expert Testimony at deposition, Annapolis, MD (January 18 & 19, 2023).
- Meta Platforms, Inc. vs. **Sitnet LLC**, IPR2024-00529, IPR2024-00530, IPR2024-00528, IPR2024-00612, Hecht Partners, US Patent Trial and Appeal Board. (Patent Validity)
  - Expert Testimony at deposition, Austin, TX (February 7, 2025).
- **US Dominion, Inc**.. vs. Newsmax Media Inc, Case # N21C-08-063 EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
  - Expert Testimony at deposition, West Palm Beach, FL (February 4, 2025).

- Dr. Rachel Kent, Class Representative vs. **Apple Inc, Apple Distribution International Limited**, Case # 1403/7/7/21, Gibson Dunn, Competition Appeal Tribunal, London, England. (App Store Security & Privacy)
  - Expert Testimony at Trial, London, England (January 27-28, 2025).
- **Virtru Corporation** vs Microsoft Corporation, Case #1:22-cv-01309-DAE; Morrison & Foerster, United States District Court, Western District of Washington.
  - Expert Testimony at deposition, Stuart, FL (December 20, 2024). (Patent Secondary Consideration and Non-infringing alternatives)
  - Expert Testimony at deposition, Stuart, FL (December 19, 2024). (Patent infringement)
- Google LLC vs. **Security First Innovations**, IPR 2024-00212, IPR 2024-00214, IPR 2024-00215, Sullivan & Cromwell, US Patent Trial and Appeal Board. (Patent Validity)
  - Expert Testimony at deposition, Stuart, FL (December 12, 2024).
- Datavant, Inc vs. **Vigilitics, LLC**, IPR 2024-00226, Fish & Richardson, US Patent Trial and Appeal Board. (Patent Validity)
  - Expert Testimony at deposition, Stuart, FL (November 22, 2024).
- **Proxense, LLC**, vs. Google., Case # 6:23-cv-00320-ADA; Susman Godfrey, United States District Court, Western District of Texas.
  - Expert Testimony at deposition, Annapolis, MD (October 23, 2024), (Patent Validity)
  - Expert Testimony at deposition, Annapolis, MD (October 22, 2024), (Patent infringement)
  - Expert Testimony at deposition, Key West, FL (December 18, 2023), (Patent claim construction)
- Robocast vs. **Netflix Inc**, Case # 1:22-cv-00305-JLH-CJB, Latham & Watkins, United States District Court, District of Delaware. (patent Non-infringement and patent invalidity)
  - Expert Testimony at Deposition, Washington DC, (August 28, 2024).
- Epic Games, Inc & Anor vs. **Apple Inc & Anor**., Case # NSD 1236 of 2020, Gibson Dunn, Federal Court of Australia, District of New South Wales. (App Store Security & Privacy)
  - Expert Testimony at Trial, Melbourne, Australia (May 29, 2024).
- **Softex LLC** vs Absolute Software Corporation, Dell Technologies Inc, and HP Inc, Case # 1:22-cv-01309-DAE; McKool Smith, United States District Court, Western District of Texas. (Patent Claim Construction)
  - Expert Testimony at deposition, Key West, FL (November 27, 2023).
- **Milliman, Inc** and Vigilytics LLC, vs. Gradient A.I. Corp., Case # 1:21-cv-10865-NMG; K&L Gates, United States District Court, District of Massachusetts. (Patent Claim Construction, Patent Infringement, Patent Validity, Trade Secret)
  - Expert Testimony at deposition, Annapolis, MD (November 27, 2023).
  - Expert Testimony at deposition, Annapolis, MD (November 17, 2022).
- Microsoft Corporation vs. **Mediapointe, Inc**, Case # 2:22-cv-01009-MCS-MRW; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
  - Expert Testimony at deposition, Annapolis, MD (September 29, 2023).

- Akamai Technologies, Inc vs. **Mediapointe, Inc**, Case # 2:22-cv-06233-MCS-AFM; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
  - Expert Testimony at deposition, Annapolis, MD (September 22, 2023).
- Lauri Valjakka vs. **Netflix Inc**, Case # 4:22-cv-01490-JST, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
  - Expert Testimony at Deposition, Annapolis, MD (September 8, 2023).
- **TecSec Inc** vs. Oracle, Case # 1:10CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
  - Expert Testimony at deposition, Annapolis, MD (June 13, 2023).
  - Expert Testimony at deposition, Annapolis, MD (September 11, 2020).
- Global Eticket Exchange Ltd. vs. **TicketMaster LLC**, Case # 6:21-cv-00399-ADA, Fish & Richardson, United States District Court, Western District of Texas. (Patent Non-infringement and validity)
  - Expert Testimony at Trial, Waco, TX (May 3, 2023).
  - Expert Testimony at Deposition, Annapolis, MD (January 31, 2023).
  - Expert Testimony at Deposition, Annapolis, MD (January 16, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01306, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
  - Expert Testimony at deposition, Annapolis, MD (April 20, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01307, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
  - Expert Testimony at deposition, Annapolis, MD (April 19, 2023).
- **TecSec Inc** vs. Cisco, Case # 1:10-CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
  - Expert Testimony at deposition, Washington DC (April 12, 2023).
  - Expert Testimony at deposition, Annapolis, MD (September 14, 2020).
- Finjan vs. **Palo Alto Networks**, Case # 4:14-CV-04908-PJH, Morrison and Foerster, United States District Court, Northern District of California.
  - Expert Testimony at Deposition, Annapolis, MD (March 17, 2022). (*Patent Non-infringement and invalidity)*
  - Expert Testimony at Deposition, Annapolis, MD (March 15, 2022). *Patent Non-infringement and invalidity)*
  - Expert Testimony at Deposition, Pikesville, MD (August 16, 2021). (*Claim Construction)*
- Centripetal Networks, Inc. vs. **Keysight Technologies, Inc.**, Investigation No. 337-TA-1314-MJM, Reed Smith LLP, United States International Trade Commission (ITC). (Patent Non-infringement & Domestic Industry Technical Prong)
  - Expert Testimony at Trial, Washington DC (March 6, 2023).
  - Expert Testimony at Deposition, Las Vegas, NV (December 2, 2022).
- **Proxense, LLC**, vs. Samsung Electronics Co., Case # 6:21-cv-00210ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
  - Expert Testimony at deposition, Annapolis, MD (January 12, 2023).
  - Expert Testimony at deposition, Annapolis, MD (September 30, 2022).

    - Expert Testimony at deposition, Annapolis, MD (September 29, 2022).
- **US Dominion, Inc**.. vs. Fox News Network, Case # N21C-03-257-EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
    - Expert Testimony at deposition, Annapolis, MD (January 10, 2022).
- **Rimini Street, Inc**. vs. Oracle International Corporation, et. al., Case # 2:14-CV-01699 LRHCWH, Gibson Dunn, United States District Court, District of Nevada. (Software security)
    - Expert Testimony at trial, Las Vegas, NV (December 9, 2022).
    - Expert Testimony at deposition, Baltimore, MD (August 30, 2018).
- **IOEngine, LLC**, vs. Ingenico Inc., Case # 1:18-cv-826 WCB; Dechert LLP, United States District Court, District of Delaware. (Patent Infringement & Patent Validity)
    - Expert Testimony at trial, Wilmington, DE (July 12 & 14, 2022).
    - Expert Testimony at deposition, Annapolis, MD (January 28, 2022).
    - Expert Testimony at deposition, Bonita Springs, FL (January 19, 2022).
- **WSOU Investments, LLC**, vs. Microsoft Corporation, Case # 6:20-cv-00464-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
    - Expert Testimony at deposition, Annapolis, MD (May 15 & 16, 2022).
- **10Tales Inc.** vs. TikTok PTE. LTD., Case # 4:21-cv-3868-YGR; Cozen O'Connor, United States District Court, Northern District of California. (Patent Claim Construction)
    - Expert Testimony at deposition, Annapolis, MD (May 11, 2022).
- **IOEngine, LLC**, vs. PayPal Holdings, Inc., Case # 1:18-cv-452-WCB; Dechert LLP, United States District Court, District of Delaware. (Patent infringement)
    - Expert Testimony at deposition, Bonita Springs, FL (January 18, 2022).
    - Expert Testimony at deposition, Bonita Springs, FL (January 26, 2022).
- AGIS Software Development LLC vs. **Uber Technologies Inc**., Case # 2:21-cv-00026-JRG-RSP, Gibson Dunn, United States District Court, Eastern District of Texas. (Non-infringement)
    - Expert Testimony at Deposition, Annapolis, MD (December 22, 2021).
- Sable Networks vs. **Splunk Inc.,** Case # 5:21-CV-00040-RWS, Morrison and Foerster, United States District Court, Eastern District of Texas. (Claim Construction)
    - Expert Testimony at Deposition, Annapolis, MD (December 13, 2021).
- Huawei Technologies Co. vs. **Verizon Communications Inc**., Case # 6:20-CV-00090, Quinn Emanuel, United States District Court, Western District of Texas. (Patent Non-infringement and patent invalidity)
    - Expert Testimony at Deposition, Pikesville, MD (July 1, 2021).
- Epic Games, Inc. vs. **Apple Inc**., Case # 4:20-cv-05640-YGR-TSH, Gibson Dunn, United States District Court, Northern District of California. (Sherman Act)
    - Expert Testimony at Trial, Oakland, CA (May 20-21, 2021).
    - Expert Testimony at Deposition, Pikesville, MD (March 26, 2021).
- Philips North America LLC ; Koninklijke Philips N.V. vs. **Summit Imaging Inc**., Case # 2:19cv01745JLR, Seed IP, United States District Court, Western District of Washington at Seattle. (DMCA and Copyright)
    - Expert Testimony at deposition, Pikesville, MD (March 16, 2021).

- **California Physicians Service, Inc D/B/A Blue Shield of California** vs. Healthplan Services Inc, Case # 3:18-cv-3730 Latham & Watkins, United States District Court, Northern District of California. (Contract Dispute: Software Quality and Security)
  - Expert Testimony at Deposition, Pikesville, MD (March 9, 2021).
- Finjan vs. **Qualys Inc**., Case # 4:18-cv-07229-YGR, Wilson Sonsini, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
  - Expert Testimony at Deposition, Pikesville, MD (March 4, 2021).
- Finjan vs. **Sonicwall Inc**., Case # 5:17-cv-04467-BLF-HRL, Duane Morris, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
  - Expert Testimony at deposition, Pikesville, MD (October 30, 2020).
  - Expert Testimony at deposition, Pikesville, MD (October 29, 2020).
- **Blackberry Limited** vs. Facebook, Inc, Case #2:18-cv-01844 (KSx), Quinn Emanuel Urquhart & Sullivan, LLP, United States District Court, Central District of California. Expert Testimony at Deposition, Baltimore, MD (December 20, 2019). (patent infringement & patent validity)
- **Netfuel, Inc**. vs. Cisco Systems, Inc, Case # 5:18-cv-2352-EJD, Susman Godfrey, United States District Court, Northern District of California.
  - Expert Testimony at Deposition, Baltimore, MD (December 16 & 17, 2019). (patent infringement & patent validity)
  - Expert Testimony at Deposition, Baltimore, MD (June 11, 2019). (patent infringement)
  - Expert Testimony at Markman Hearing, San Jose, CA (February 28, 2019). (courtroom tutorial)
  - Expert Testimony at deposition, Baltimore, MD (December 20, 2018). (claim construction)
- **Symantec Corporation** vs. Zscaler, Inc., Case # 3:17-CV-04414-JST, Baker Botts, United States District Court, Northern District of California.
  - Expert Testimony at Deposition, Baltimore, MD (December 6, 2019). (patent infringement)
  - Expert Testimony at Deposition, Baltimore, MD (August 2, 2019). (Assignor Estoppel)
- Koninklijke Philips vs. **Microsoft Inc**, Case # 4:18-cv-01885-HSG, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
  - Expert Testimony at Deposition, Baltimore, MD (July 17, 2019).
- **Cypress Lake Software**, Inc. vs. Samsung Electronics & Dell Inc, Case # 6:18-cv-030-JKD and 6:18cv0138JDK, Garteiser Honea, United States District Court, Eastern District of Texas. (patent infringement and patent validity)
  - Expert Testimony at Deposition, Baltimore, MD (July 1011, 2019).
- Finjan vs. **Juniper Networks**, Case # 3:17-cv-05659-WHA , Irell and Manella, United States District Court, Northern District of California.
  - Expert Testimony at deposition, Baltimore, MD (April 2, 2019). (patent Non-infringement)

    - Expert Testimony at deposition, San Francisco, CA (March 9, 2019). (patent Non-infringement)
    - Expert Testimony at trial, San Francisco, CA (December 13, 2018). (patent Non-infringement and invalidity)
    - Expert Testimony at deposition, Baltimore, MD (November 9, 2018). (patent Non-infringement and invalidity)
    - Expert Testimony at deposition, Baltimore, MD (July 6, 2018). (patent Non-infringement)
    - Expert Testimony at deposition, Baltimore, MD (June 12, 2018). (patent Non-infringement)
- Grace et. al. vs. **Apple Inc**., Case # 5:17-CV-00551LHK (NC), Durie Tangri, United States District Court, Northern District of California. (class action)
    - Expert Testimony at deposition, Towson, MD (September 26, 2018).
- Grace et. al. vs. **Apple Inc**., Case # 5:17-CV-00551-LHK (NC), Kirkland & Ellis, United States District Court, Northern District of California. (class certification)
    - Expert Testimony at deposition, Pikesville, MD (July 3, 2018).
- **F5 Networks, Inc**. vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
    - Expert Testimony at deposition, Baltimore, MD (January 24, 2018).
- **Amazon.com Inc., Hulu, LLC, and Netflix, Inc**, vs. Uniloc Luxembourg S.A., IPR 201700948, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
    - Expert Testimony at deposition, Baltimore, MD (October 9, 2017).
- Phishme, Inc. vs. **Wombat Technologies, Inc,** Case # 16403-LPS-CJB, K&L Gates, United States District Court, Delaware. (patent claim construction)
    - Expert Testimony at deposition, Washington DC, (October 5, 2017).
- Finjan vs. **Symantec Corporation**., Case # 14-cv-02998-HSG, Quinn Emanuel, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
    - Expert Testimony at deposition, Baltimore, MD (September 14-15, 2017).
- **Kudelski SA, Nagra USA, Inc., Nagravision SA, and OpenTV, Inc**. vs. Comcast Corporation, Case # 2:16-cv-1362-JRG, Covington, United States District Court, Eastern District of Texas. (patent claim construction).
    - Expert Testimony at deposition, Baltimore, MD (September 1, 2017).
- **F5 Networks, Inc**. vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
    - Expert Testimony at deposition, Baltimore, MD (August 10, 2017).
- Intellectual Ventures vs. **JP Morgan Chase & Co.**, Case # 1:13-cv-03777, Kirkland & Ellis, United States District Court, Southern District of New York. (Patent Non-infringement).
    - Expert Testimony at deposition, Baltimore, MD (June 1, 2017).
- Nader AsghariKamrani and Kamran AsghariKamrani vs. **United Services Automobile Association**. Case # 2:15-CV-478, Fish & Richardson, United States District Court, Eastern District of Virginia. (Patent Written Description Support related to Inequitable Conduct).
    - Expert Testimony at trial, Norfolk, VA (April 21, 2017).
    - Expert Testimony at deposition, Baltimore, MD (March 21, 2017).

- **Sabre GLBL Inc**, vs. HP Enterprise Services LLC. Case # 1310022761, JAMS Binding Arbitration Hearing, Dallas, TX (Contract dispute).
  - Expert Testimony at arbitration hearing, Dallas, TX (April 5, 2017).
- **Al Cioffi et. al.** vs. Google, Case # 2:13cv103JRGRSP, Vasquez, Benisek & Lindgren, United States District Court, Eastern District of Texas. (patent Infringement).
  - Expert Testimony at trial, Marshall, TX (February 7, 2016).
  - Expert Testimony at deposition, Baltimore, MD (September 26, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
  - Expert Testimony at deposition, Baltimore, MD (November 14, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2016-00151, Morrison & Foerster, US Patent Trial and Appeal Board. (patent Invalidity)
  - Expert Testimony at deposition, Baltimore, MD (August 19, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01974, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
  - Expert Testimony at deposition, Baltimore, MD (August 2, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-02001 & IPR 2016-00157, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
  - Expert Testimony at deposition, Baltimore, MD (July 26 & 27, 2016).
- **Amazon.com, Inc** vs. Zitovault, LLC, IPR 2016-00021, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
  - Expert Testimony at deposition, Baltimore, MD (July 22, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
  - Expert Testimony at deposition, Baltimore, MD (May 20, 2016).
- Vir2us Inc. v. **Invincea, Inc. and Invincea Labs, LLC**, Case # 2:15-cv-l62; Cooley, United States District Court, Eastern District of Virginia. (Patent Non-infringement and Invalidity)
  - Expert Testimony at deposition, Reston, VA (April 20, 2016).
- TVIIM. v. **McAfee Inc.**, Case # 3:13-cv-04545-VC; Wilmer Hale, United States District Court, District of N. California. (Patent Non-infringement and Invalidity)
  - Expert Testimony at trial, San Francisco, CA (July, 2015).
  - Expert Testimony at deposition, Baltimore, MD (February, 2015).
- Intellectual Ventures vs. **Symantec**, Case # 1:10-cv-01067-LPS; Latham & Watkins, United States District Court, District of Delaware. (Patent Invalidity)
  - Expert Testimony at trial, Wilmington, DE (February, 2015).
  - Expert Testimony at deposition, Baltimore, MD (May, 2013).
- **Rovi Solutions & Veracode** vs. Appthority, Case # 1210487-DPW; Goodwin Procter, United States District Court, District of Massachusetts. (Patent Infringement and Validity)
  - Expert Testimony at trial, Boston, MA (August 11, 2014).
  - Expert Testimony at deposition, Baltimore, MD (April 4, 2014).
- **Juniper** vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR; Irell & Manella, United States District Court, District of Delaware. (Patent Infringement)
  - Expert Testimony at trial, Wilmington, DE (February, 2014).
  - Expert Testimony in court hearing, Wilmington, DE (November 14, 2013).

    - Expert Testimony at deposition, Baltimore, MD (June, 2013).
- Prism Technologies. v. **Adobe Systems Inc.,** Case # 8:10-cv-00220-LEST-DT; DLA Piper, United States District Court, District of Nebraska. (Patent Invalidity)
    - Expert Testimony at deposition, Baltimore, MD (August, 2012).
- Finjan Inc. vs. **McAfee, Inc**., Case # 10593 (GSM), Kirkland & Ellis, United States District Court, District of Delaware. (Patent Non-infringement)
    - Expert Testimony at deposition, Washington, DC (June, 2012).
- Avaya Inc. vs. **Telecom Labs Inc,. TeamTLI.com Corp., and Continuant Technologies**, Case # 3:06-cv-02490 (GEB); K&L Gates, United States District Court, District of New Jersey. (Contract Dispute)
    - Expert Testimony at deposition, Newark, NJ (August, 2011).
- **Lear Automotive** vs. Johnson Controls Inc (JCI), Case # 04-CV-73461; Flachsbart & Greenspoon, United States District Court, Eastern District of Michigan. (Patent Infringement and Validity)
    - Expert Testimony at trial, Detroit, MI (February, 2011).
    - Expert Testimony at deposition, Baltimore, MD (December, 2005).
- **TecSec Inc** vs. International Business Machines Corporation, Case # 1:10-CV-115-LMB/TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement)
    - Expert Testimony at deposition, Newark, NJ (November, 2010).
- **Echostar Satellite Corporation** vs. NDS Group, Case # SA-CV-03950-DOC(JTL); T. Wade Welch & Associates, United States District Court, Central District of California. (Copyright and DMCA)
    - Expert Testimony at trial, Santa Ana, CA (April, 2008).
    - Expert Testimony at deposition, Santa Ana, CA (April, 2008).
    - Expert Testimony at deposition, Baltimore, MD (October, 2007).
- **Web.com Inc** vs. The Go Daddy Group Inc., Case # CV-0701552-PHX-MHM; Graves Law Office, United States District Court, Arizona. (Patent Infringement)
    - Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
    - Expert Testimony at deposition, Baltimore, MD (May, 2008).
- z4 Technologies vs. **Microsoft & Autodesk**, Case # 2:04-CV-00335-LED; Fish & Richardson, United States District Court, Eastern District of Texas. (Patent Non-Infringement and Invalidity)
    - Expert Testimony at trial, Tyler, TX, (April, 2006).
    - Expert Testimony at deposition, Washington DC (January, 2006).
- **Linda Schade** vs. Linda Lamone et. al., Trial on the Legality of Paperless Voting Machines in Maryland. (Adequacy of Voting Equipment)
    - Expert Testimony at trial, Annapolis, MD (August 25, 2004).

Awards

- 2020, **Best Paper Award**, in the category of Mobile & Wireless Computing, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- 2020, **Best Paper Award**, in the category of Image Processing & Multimedia Technology, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.

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

Four Batons EX2021
Samsung v Four Batons, IPR2025-00495
Page 101 of 101