IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS, AND NOKIA OF AMERICA CORPORATION,

Petitioners,

v.

RIGHTQUESTION, LLC,

Patent Owner.

---

U.S. Patent No. 11,005,989

Issue Date: May 11, 2021

Title: VALIDATING AUTOMATIC NUMBER IDENTIFICATION DATA

---

*Inter Partes* Review No.: IPR2025-00362

---

**DECLARATION OF DR. PATRICK MCDANIEL IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 11,005,989**

***Mail Stop* "*PATENT BOARD*"**

Patent Trial and Appeal Board

U.S. Patent and Trademark Office

P.O. Box 1450

# TABLE OF CONTENTS

**Page**


I. INTRODUCTION ..... 1

II. QUALIFICATIONS ..... 2

III. RELEVANT LEGAL STANDARDS ..... 7

IV. OVERVIEW ..... 10

V. BACKGROUND ..... 12

- A. Summary of the ’989 Patent ..... 12
- B. Claim Construction ..... 12
- C. Priority of the Challenged Claims ..... 13
- D. Person of Ordinary Skill in the Art (POSA) ..... 13

VI. State of the Art ..... 14

VII. CHALLENGED CLAIMS ..... 16

- A. Identification of Challenged Claims ..... 16
- B. Prior Art ..... 16

VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE ..... 16

- A. Ground 1: Claims 1-28 are Obvious over Har in view of Miller ..... 16
  - 1. Har ..... 16
  - 2. Miller ..... 19
  - 3. The Proposed Combination of Har and Miller. ..... 24
  - 4. Motivation to Combine the Teachings of Har and Miller ..... 32
  - 5. Detailed Application of Har in view of Miller ..... 37

a. Claim 1 ..... 37
b. Claim 2 ..... 63
c. Claim 3 ..... 65
d. Claim 4 ..... 65
e. Claim 5 ..... 66
f. Claim 6 ..... 66
g. Claim 7 ..... 67
h. Claim 8 ..... 72
i. Claim 9 ..... 72
j. Claim 10 ..... 73
k. Claim 11 ..... 75
l. Claim 12 ..... 75
m. Claim 13 ..... 77
n. Claim 14 ..... 78
o. Claim 15 ..... 78
p. Claim 16 ..... 80
q. Claim 17 ..... 81
r. Claim 18 ..... 82
s. Claim 19 ..... 82
t. Claim 20 ..... 83
u. Claim 21 ..... 84
v. Claim 22 ..... 85
w. Claim 23 ..... 86
x. Claim 24 ..... 88
y. Claim 25 ..... 90
z. Claim 26 ..... 90

aa. Claims 27 and 28. .....90

I, Dr. Patrick McDaniel, declare as follows:

## I. INTRODUCTION

1. I am over the age of eighteen (18) and otherwise competent to make this declaration.

2. I have been asked by counsel for AT&T Services Inc., Cellco Partnership d/b/a Verizon Wireless, and Nokia of America Corporation ("Petitioners") to provide an opinion concerning certain claims of U.S. Patent No. 11,005,989 ("the "'989 Patent" or the "Asserted Patent"). Specifically, I have been asked to analyze the Asserted Patents with respect to the prior art and validity requirements to render an opinion as to the validity of claims 1-28 of the '989 Patent (the "Challenged Claims"). This document presents the opinions I have formed at this time. If asked, I will testify based upon my study of these materials, as well as my own previous knowledge and experience on this subject.

3. I make the following statements based on my own personal knowledge, my experience, and my analysis of the Asserted Patents, as well as the materials I reviewed as set forth in Appendix A to this report. I understand that I may be provided additional information as this case proceeds. Accordingly, I reserve the right to change or augment my analysis and opinions in light of any new information or evidence that is presented after my report.

4. My compensation rate for this case is $750 per hour, plus reimbursement for any reasonably incurred expenses associated with my work and testimony in this case. My compensation is in no way contingent upon my performance, the outcome of this litigation, or any issues involved in or related to this litigation. I have no financial interest in the outcome of this litigation or the specifics of my opinions or judgement on any aspects in this case. I am over 21 years of age and am legally competent to testify. If called as a witness, I could and would testify to the following.

## II. QUALIFICATIONS

5. My qualifications to testify about the Asserted Patent, relevant technology, and the prior art are set forth in my curriculum vitae ("CV"), which is attached as Appendix B. My CV also includes a list of my publications and the cases in which I have testified at deposition, hearing, or trial within the past four years. As set forth in my CV:

6. I earned my Ph.D. in Computer Science from the Computer Science and Engineering Department at University of Michigan, Ann Arbor in 2001. I earned my Bachelor of Science degree in Computer Science from Ohio University

in 1989, and my Master of Science degree, also in Computer Science, from Ball State University in 1991.

7. Since 2022, I have been Tsun-Ming Shih Professor of Computer Sciences in the School of Computer, Data and Information Sciences at the University of Wisconsin-Madison. Prior to my move to Wisconsin, I was the William L. Weiss Professor of Information and Communications Technology in the School of Electrical Engineering and Computer Science at the Pennsylvania State University in University Park, PA. I was also the director of the Institute for Network and Security Research, and founder and co-director of the Systems and Internet Infrastructure Security Laboratory, a research laboratory focused on the study of security in diverse network and computer environments. My research efforts primarily involve computer systems, network management and authentication, systems security, and technical public policy.

8. I frequently teach and do research on cellular and telephony systems, particularly as it relates to security. For example, I was recently awarded "Most Influential Paper of PLDI", which is a conference on Programming Language Design and Implementation, for my pioneering work on the security of cellular systems. I continue to do research in cellular security research to this day.

9. Prior to 2017, I was an Assistant Professor (2004-2007), Associate Professor (2007-2011), Full Professor (2011-2015), and Distinguished Professor (2016-2017) of Computer Science and Engineering and the William L. Weiss Professor of Information and Communications Technology (2017-2022) at the Pennsylvania State University. Since 2004, I have taught courses in the field of computer systems, systems programming, mobile device security, networks, and network and computer security at both the undergraduate and graduate level. I created and maintained several of these courses at Penn State University. I have begun teaching courses at the University of Wisconsin-Madison in the Fall of 2023, including courses such as network and systems security.

10. From 2003-2009, I was an Adjunct Professor at the Stern School of Business at New York University in New York, NY. At the Stern School of Business, I taught courses in computer and network security and online privacy.

11. I am a Fellow of the Association for Computing Machinery (ACM, the leading professional association for computer science), a Fellow Institute for Electrical and Electronics Engineering (IEEE, the leading professional association for engineering), and Fellow of the American Association for the Advancement of Science (AAAS, the leading professional association for science).

12. I am the director of the NSF Frontier Center for Trustworthy Machine Learning (CTML), a research organization exploring security and privacy of machine learning (and AI in general). Funded by the US National Science Foundation, the CTML is led by the University of Wisconsin-Madison and has members from Stanford, the University of California, Berkeley, The University of California-San Diego, and the University of Virginia.

13. I was the Program Manager (PM) and lead scientist for the Cyber Security Collaborative Research Alliance (CRA). The CRA is led by Penn State University and includes faculty and researchers the Army Research Laboratory, Carnegie Mellon University, Indiana University, the University of California-Davis, and the University of California-Riverside. This initiative is a major research project aimed at developing a new science of cyber-security for military networks, computers, and installations.

14. I have served as an advisor to several Ph.D. and master's degree candidates, several of whom have gone on to become professors at various institutions such as North Carolina State University, Purdue University, the University of Toronto, the University of Oregon, and the Georgia Institute of Technology and the University of Florida. I am currently an advisor to seven Ph.D. students.

15. Before joining Pennsylvania State University as a professor, I was a software developer and project manager for companies in the networking industry including Applied Innovation, Inc., and Primary Access Corporation. I was also a senior researcher at AT&T Research-Labs. As part of my duties in these industrial positions, I informed, reviewed, and formed corporate policies and practices relating to the security of mobile devices, networks, and software systems (including filesystems).

16. I have published extensively in the field of mobile security, network and security management, computer systems, authentication, storage and filesystems, systems security, applied cryptography and network security. In addition to writing several articles for industry journals and conferences, I have authored portions of numerous books related to computer systems, applied cryptography and network security. I have served on the editorial boards of several peer-reviewed journals including ACM Transactions on Internet Technology, for which I was the Editor-in-Chief. I was also an Associate Editor for ACM Transactions on Information and System Security and IEEE Transactions of Software Engineering, two highly regarded journals in the field.

17. Additional information regarding my background, qualifications, publications, and presentations is provided in my CV, attached as Appendix B to this report.

## III. RELEVANT LEGAL STANDARDS

18. I am not a lawyer and do not provide any legal opinions in this Declaration. Although I am not a lawyer, I have been informed and understand that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims. I have been asked to provide my opinions regarding whether the claims of the '989 Patent are anticipated or would have been obvious to a person having ordinary skill in the art at the time of the alleged invention, in light of the prior art.

19. I have been informed and understand that a patent claim is not patentable under 35 U.S.C. § 103 if the differences between the patent claim and the prior art are such that the claimed subject matter as a whole would have been obvious at the time the claimed invention was made to a person having ordinary skill in the relevant art. Obviousness, as I have been informed and understand, is based on the scope and content of the prior art, the differences between the prior art and the claim,

the level of ordinary skill in the art, and, to the extent that they exist, certain objective indicia of non-obviousness.

20. I understand that objective indicia can be important evidence regarding whether a patent is obvious or nonobvious, if it has an appropriate nexus to the claimed invention, i.e., is a result of the merits of a claimed invention (rather than the result of design needs or market-pressure advertising or similar activities). Such indicia include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeded contrary to the accepted wisdom of the prior art.

21. I have been informed that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the relevant art at the time of the invention. As such, my opinions below as to a person of ordinary skill in the art are as of the time of the invention, even if not expressly stated as such; for example, even if stated in the present tense.

22. In analyzing the relevance of the differences between the claimed invention and the prior art, I have been informed that I must consider the impact, if any, of such differences on the obviousness or non-obviousness of the invention as a whole, not merely some portion of it. The person of ordinary skill faced with a problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

23. I have been informed that a precise teaching in the prior art directed to the subject matter of the claimed invention is not needed. I have been informed that one may take into account the inferences and creative steps that a person of ordinary skill in the art would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a person of ordinary skill in the art at the time of the invention, then this evidence would make it more likely that the claim was obvious. On the other hand, if the combination of known elements yielded unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious.

24. I have been informed and understand that there are recognized, exemplary, rationales for combining or modifying references to show obviousness of claimed subject matter. Some of the rationales include the following: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to yield predictable results; use of a known technique to improve a similar device (method or product) in the same way; applying a known technique to a known device (method or product) ready for improvement to yield predictable results; choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art teachings to arrive at the claimed invention.

## IV. OVERVIEW

25. Claims 1-28 of the ’989 Patent (the “Challenged Claims”) are unpatentable as obvious over the prior art. The claims are directed to receiving a

device information value and a score indicating validity of a phone number. A security determination is then performed based on that data. Ex-1001, 2:46-62.

26. Allowance of the Challenged Claims was based solely on an amendment related to conveying an assurance or failure to the callee after the security determination has been made. *See* Ex-1002, 392.

27. Consistent with the Examiner's rejection, using device information and generating values and scores to assist in making a security determination was well-known. Conveying an assurance to the callee about the security determination was also well known.

28. The Challenged Claims thus recite nothing more than a combination of prior art elements, each used for its normal and intended purpose, that were well-known obvious modifications to a POSA.

29. A POSA was familiar with the state of the art and was motivated to modify and combine the teachings in the prior art identified in the Grounds below to establish that the Challenged Claims recite nothing more than a combination of prior art elements, each used for its normal and intended purpose, and thus the recited limitations are an obvious modification of the cited prior art.

## V. BACKGROUND

### A. Summary of the ’989 Patent

30. The ’989 Patent describes “techniques for ascertaining the identity of a device initiating communications” to detect “potential attempts at spoofing of caller ID or automatic caller identification (ANI) data.” Ex-1001, 2:42-58.

31. To address caller identification spoofing, the ’989 Patent describes analyzing a caller’s device information to generate a score indicating the validity of the phone number. Ex-1001, [8:61-9:54]. Based on the caller’s device information and the generated score, a security determination is made (*e.g.*, “blocking access”). *Id*. 9:51-54.

### B. Claim Construction

32. I have been informed and understand that in order to properly evaluate the ’989 Patent, the terms of the claims must first be interpreted.

33. I understand that Petitioner proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction. The plain meaning is the ordinary and customary meaning to those skilled in the art.

### C. Priority of the Challenged Claims

34. For purposes of this *inter partes* review, I have been instructed to assume that the priority date is November 7, 2013.

### D. Person of Ordinary Skill in the Art (POSA)

35. I am familiar with the knowledge and capabilities of one of ordinary skill in the art. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of November 7, 2013.

36. I have been informed and understand that a Person of Ordinary Skill in the Art ("POSA") is a hypothetical person who is presumed to be aware of all pertinent prior art, thinks along conventional wisdom in the art, and is a person of ordinary creativity.

37. With respect to the '989 Patent, a POSA in November 2013 would have been familiar with security of cellular/telephony networks and mobile systems. A POSA would have had at least a Bachelor's degree in computer science, electrical engineering, or a related technical field, and at least two years of professional experience, or an equivalent advanced education, in the field in security of cellular/telephony networks and mobile systems. Additional work experience in

relevant industries could compensate for less education or education in a different field, and vice versa.

38. A POSA may work as part of a multi-disciplinary team and draw upon not only his or her own skills, but also take advantage of certain specialized skills of others on the team to solve a given problem.

## VI. STATE OF THE ART

39. The following section describes the state of the art as of the priority date of the ’989 Patent. The prior art references, and the discussions of what was known to a POSA, provide the factual support for the general description of the state of the art at the time of the invention, provide additional motivation to modify or combine the reference. Accordingly, these references should be considered by the Board.

40. As the Examiner identified during prosecution, receiving information pertaining to a call, to include a value associated with the calling device and a score indicating validity of the call, were well known in the art. Ex-1002, 279-289. *See e.g.,* Ex-1011, 46; Ex-1012, 384-385, Ex-1013, 4-5, Ex-1014, 4-7, Ex-1005, Ex-1006.

41. The Applicant did not dispute the Examiner's conclusion and Allowance of the Challenged Claims during prosecution was based solely on an amendment related to conveying an assurance or failure to the callee after the security determination is made.

42. However, prior to the earliest priority date for the '989 Patent, conveying the results of a security determination based on device information and a score were well-known in the art.

43. For example, Schwartz discloses that the subscriber may be notified about whether a call is suspicious in the form of "a text message or iconic indication may be provided for display by the UA device." Ex-1005, [0149]. As another example, Har discloses "a message indicating success or failure of authentication can be prepared and sent to the second user, the user receiving the authentication results." Ex-1004, [0018].

44. A POSA was familiar with the state of the art and was motivated to modify and combine the teachings of the prior art cited in the Grounds below to create a more robust and secure authentication system to establish that the Challenged Claims recite nothing more than a combination of prior art elements, each used for its normal and intended purpose, and thus the recited limitations are an obvious modification of the cited prior art.

## VII. CHALLENGED CLAIMS

### A. Identification of Challenged Claims

45. Based on my understanding of the law of obviousness discussed above Claims 1-28 of the ’989 Patent are invalid as obvious over Har in view of Miller.

| Ground | Claim(s) | Basis | Reference |
|---|---|---|---|
| 1 | 1-28 | §103 | Har in view of Miller |

### B. Prior Art

46. I have been informed that Har (U.S. Patent Publication No. 2012/0144198) and Miller (U.S. Patent Publication No. 2012/0201381) qualify as prior art under §§ 102(a)(1).

## VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

### A. Ground 1: Claims 1-28 are Obvious over Har in view of Miller

#### 1. Har

47. Har teaches a call authentication system using a data channel and an authentication server to “authenticate the identity of one or more parties to a call where at least one of the parties to the call is using a mobile device.” Ex-1004, Abstract. Har’s “authentication methodology can be used … to authenticate a first user to a second user by authenticating a message sent by the first user to the

authentication server." Ex-1004, [0002]. "The message can include the identity of the first user and other information." *Id.* Notably, Har's authentication request "can be encrypted and/or signed and sent over a data channel." *Id.* "In response to successful validation by the authentication server, the authentication server can send an authentication indication to the device of the user receiving the authentication results" which "can display identification information … associated with the" caller *Id.*

48. Har's Fig. 1 illustrates authentication in a mobile environment. Ex-1004, [0006], [0022]. As shown in Fig. 1, "a first user can be a caller such as caller 114 using a caller mobile device." Har's "[c]aller 114 … can authenticate his identity to callee 116 … by sending an authentication request to … authentication server 102." Ex-1004, [0023]. "The authentication request can include information identifying the caller 114, information identifying the callee 116, any other information that caller 114 would like callee 116 to have and/or any other information that caller 114 specifies." *Id.* "An authentication server … can decrypt the encrypted request using the server's public key and the digital signature can be verified using the public key of the user sending the message." Ex-1004, [0026]. "The message can include information associated with the first user, as registered in

the server's database, and any other data sent in the authentication request." Ex-1004, [0035].

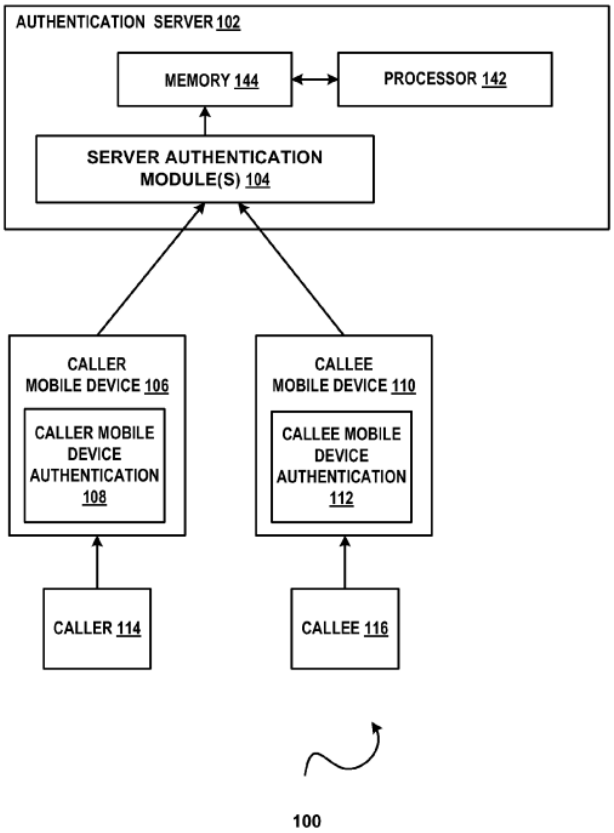



**FIG. 1**

***Har – Fig. 1***

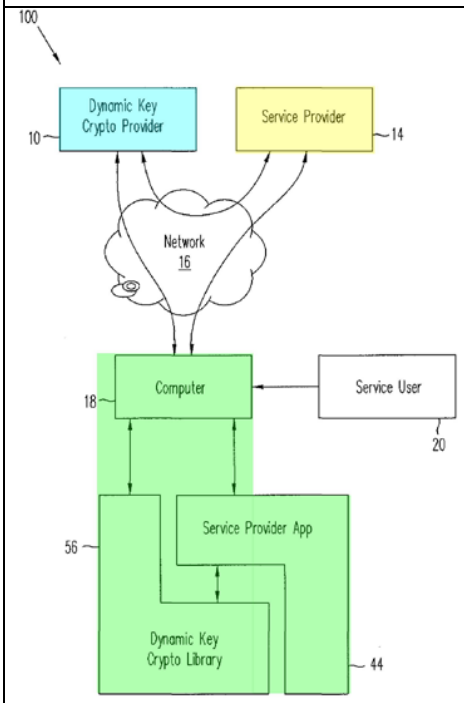
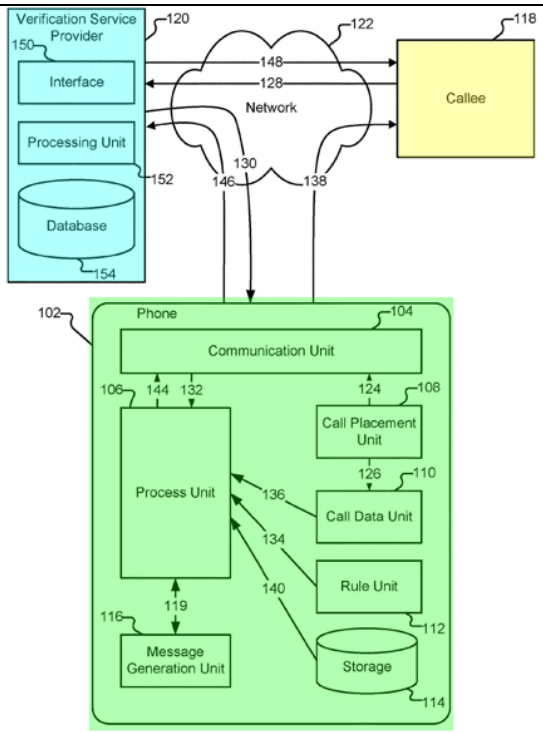
49. Har's "authentication server may have a data store of user information that includes the mobile telephone numbers of users, usernames, passwords, PIN codes, the name, address and public keys for users, credentialing information,

identification information and so on." Ex-1004, [0018]. Har's system "supports authentication of mobile devices." Ex-1004, [0044].

**2. Miller**

50. Miller describes a system for authorizing / verifying a device involved in a communication that heavily overlaps with the (later) '989 patent system. For such verification, Miller "uniquely identif[ies] the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device." Ex-1022, Abstract.

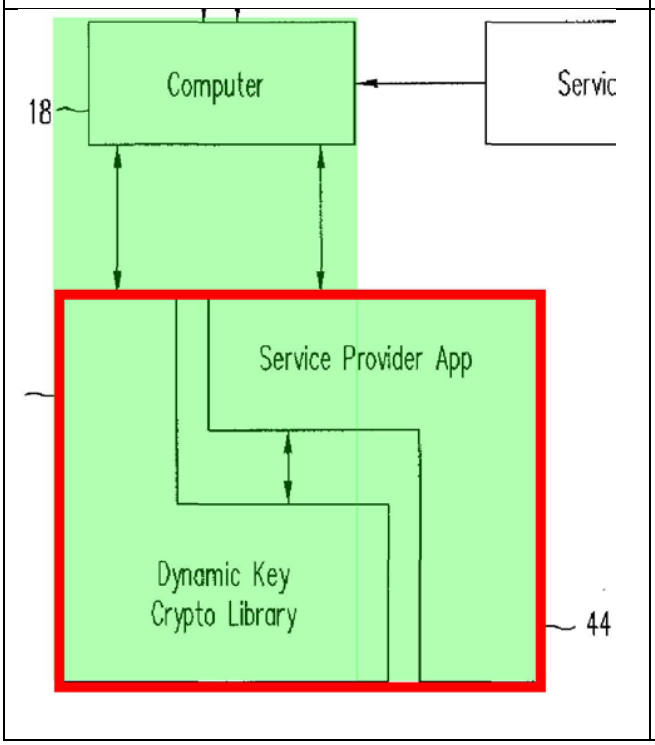
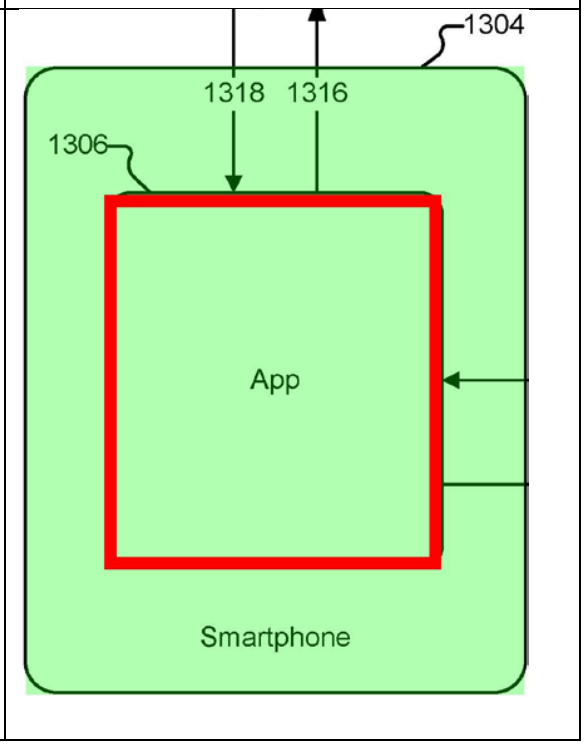
51. The '989 patent adopted (and claimed) an architecture and processes largely matching Miller's disclosure. For example, Figures 1 from each of Miller and the '989 patent shows the matching relevant components in the communication.

| Miller (Ex-1022) | ’989 Patent (Ex-1001) |
|---|---|
|   FIG. 1 |   FIG. 1 |

Miller and the ’989 patent each teach communication between a first device (green) and a second device (yellow) for which the “first device” is authorized / verified by a verification provider (blue) which Miller calls a “dynamic key crypto provider” (herein, “DKCP”) and the ’989 patent calls a “verification service provider” (herein, “VSP”).

52. Miller and the ’989 patent describe the same types of “devices” in the communication. Compare Ex-1022, [0048] and Ex-1001, 12:26-31.

53. Miller and the ’989 patent both teach that an “app” may be used on the device to facilitate verification.

| Miller (Ex-1022, Fig. 1) | ’989 Patent (Ex-1001, Fig. 13 |
|---|---|
|   |   |

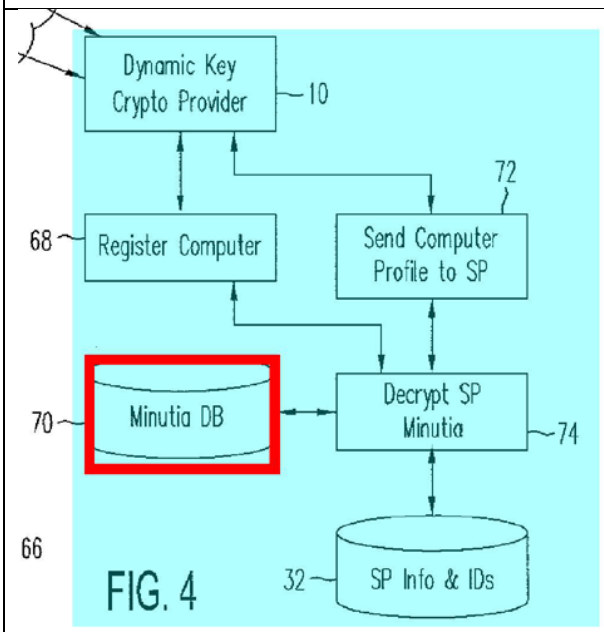
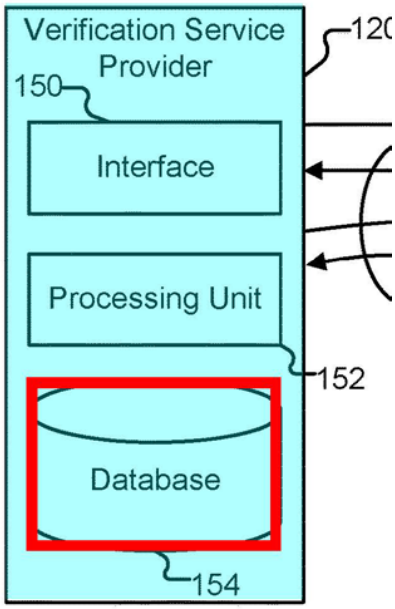
Compare Ex-1022, [0048], Ex-1001, 5:60-63.

54. Miller’s DKCP and the ’989 patent VSP are both implemented as computer servers using the typical server hardware such as processors, memories and software. Ex-1022, [0177-0179]; Ex-1001, 4:5-22.

55. Miller teaches the same functional steps that the ’989 patent later regurgitated. First, both Miller and the ’989 patent register devices with the

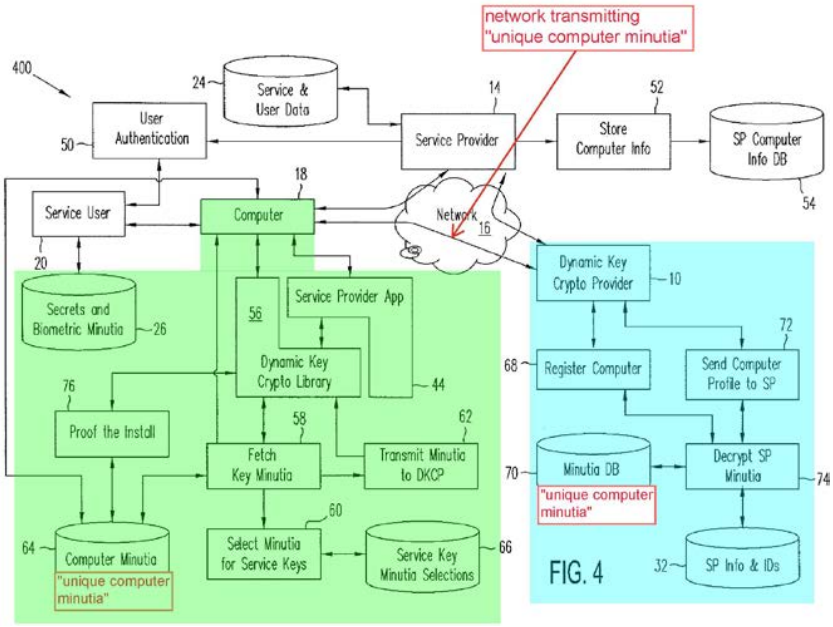
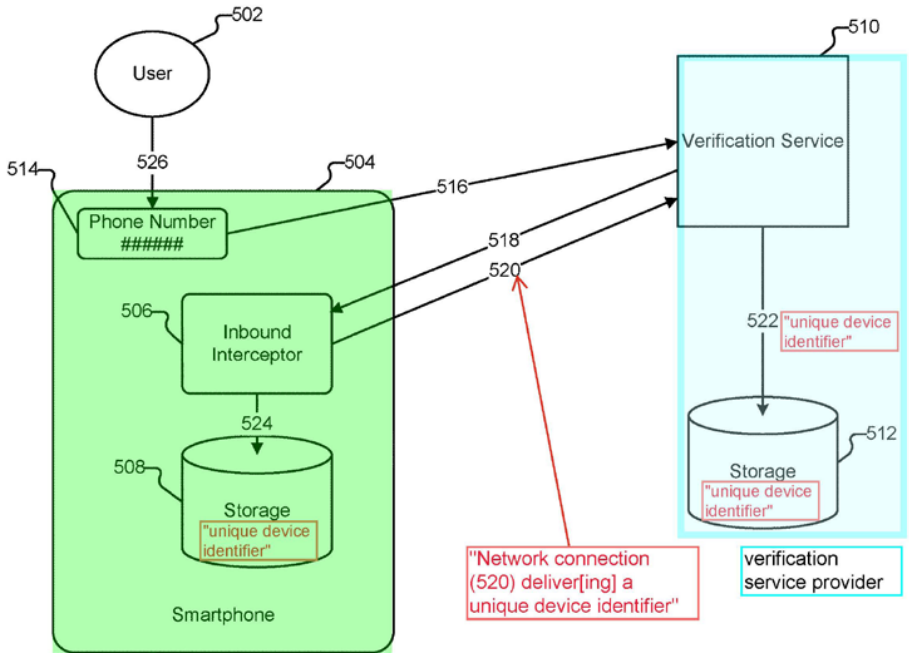
DKCP/VSP using unique device identifiers – which Miller calls "computer minutia" or "computer fingerprints" and the '989 calls a "device fingerprint."

56. Second, both Miller's DKCP and the '989 patent VSP store the enrolled device information (fingerprint/minutia) in databases for later usage.

| **Miller (Ex-1022, Fig. 4)** | **'989 Patent (Ex-1001, Fig. 1)** |
|---|---|
|   |   |

Compare Ex-1022, [0092], Ex-1001, 3:65-67.

57. Third, both Miller's DKCP and the '989 patent VSP receive a device information (minutia) from the device during authentication.

| | |
|---|---|
| **Miller (Ex-1022, Fig. 4)** |  |
| **'989 Patent (Ex-1001, Fig. 5)** |  |

58. Fourth, both Miller's DKCP and the '989 patent VSP compare the registered minutia / enrolled fingerprint against the minutia / fingerprint received from a device seeking authentication. Compare Ex-1022, [0066], Ex-1001, 9:24-26.

59. Fifth, both Miller's DKCP and the '989 patent VSP teach calculating a "score" based upon the device's information (and enrollment information) and various other factors to help determine authenticity. Compare Ex-1022, [0105], Ex-1001, 9:39-45.

60. Sixth, both Miller's DKCP and the '989 patent VSP select actions, such as blocking (denying) communication, allowing communication, or seeking further information, such as PIN's or passwords from the users. Compare Ex-1022, [0112-0116], Ex-1001, 9:55-59.

61. Simply put, Miller discloses the same architecture and functionality that the '989 patent subsequently disclosed and claimed.

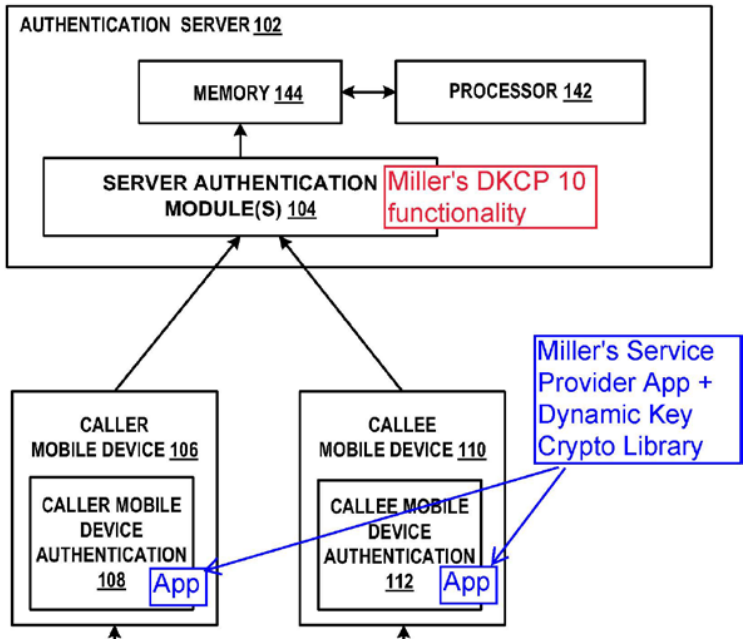
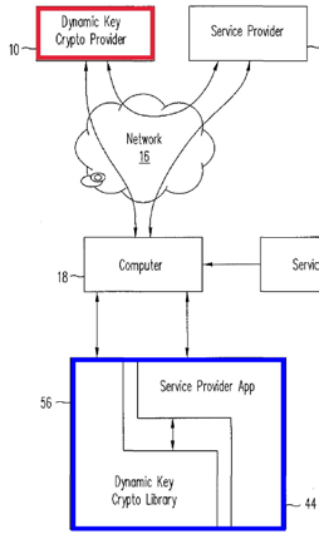
### 3. The Proposed Combination of Har and Miller.

62. As noted in the Introduction, when read reasonably, Har teaches or renders obvious the system claimed in the '989 patent but does not expressly recite the term "score" to describe its security determination. However, Har teaches a security determination based on two factors. Miller provides explicit details

regarding both factors of Har's security determination including using a "score" system for verification / authentication of devices.

63. The proposed combination augments Har's existing authentication system to include the functionality of Miller's authentication system specific to device authentication and, more particularly, to include Miller's score authentication as one basis for Har's two-factor security determination.

64. As shown below, this augmentation includes (1) incorporating aspects of Miller's DKCP server 10 functionality into Har's "authentication server 102"; and (2) incorporating Miller's DKCP client app functionality ("service provider app 44" and "dynamic key crypto library 56" which may be combined into one program as per Ex-1022, [0072], [0048]) into Har's "Mobile Device Authentication Modules" 108 and 112.

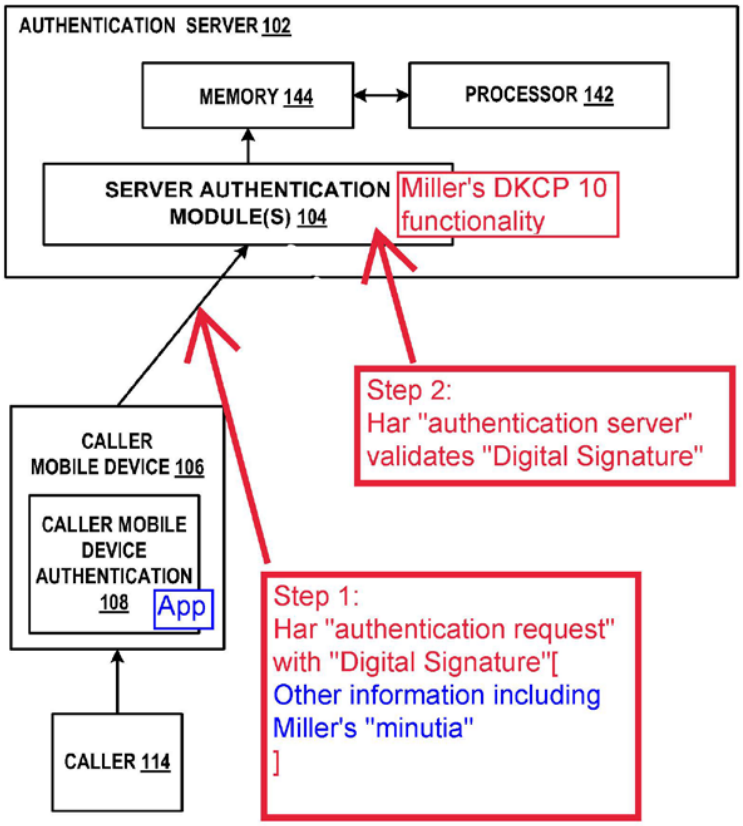
| Ex-1004, Fig. 1 | Ex-1022, Fig. 1 |
|---|---|
|  |  |



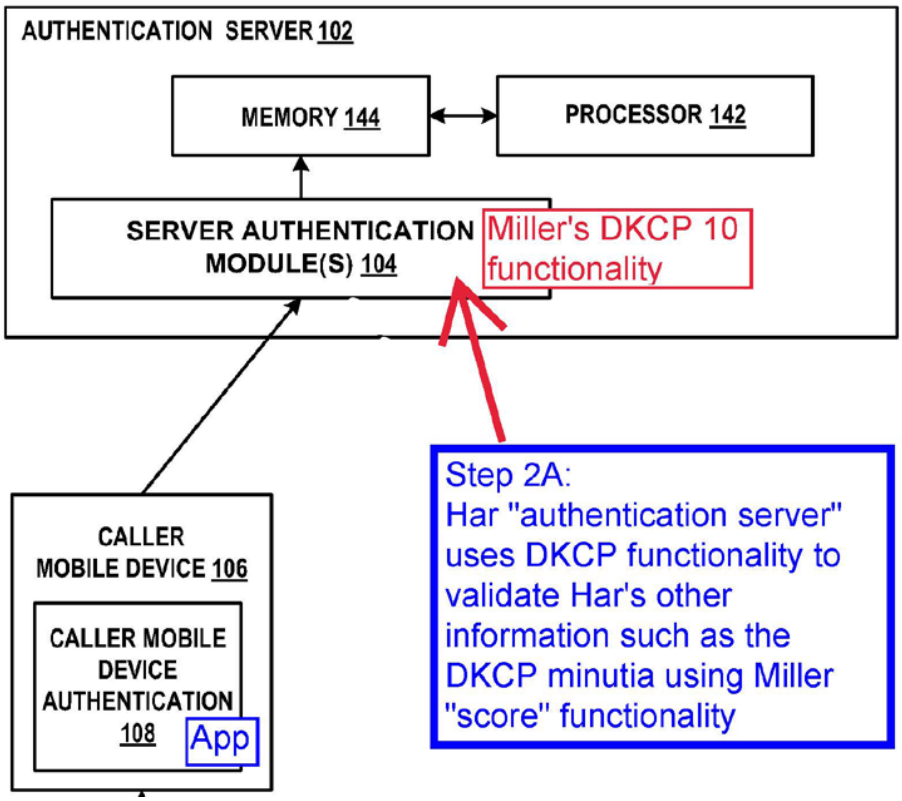
65. The Har/Miller System uses Har's basic authentication flow augmented by Miller's DKCP functionality. *E.g.*, Ex-1004, Fig. 2; elements 1.ii-1.iv *infra*.

66. **Step 1 (adopted directly from Har)**: The caller sends an "authentication request [of] a message encrypted using the server's public key … and signed using the private key …" Ex-1004, [0016]. The "authentication request [] includes" other forms of "identification information associated with the authentication request sender" or "information volunteered by the authentication request sending" or "desired by the requesting user." Ex-1004, [0016].

67. In the Har/Miller System, the authentication request identification information includes "minutia" that Miller's DKCP system uses for device-based authentication. *See* Section VII.A.2 (*supra*), elements 1.ii, 1.iii (*infra*).




68. **Step 2 (adopted directly from Har)**: Har's authentication server attempts to validate / authenticate the request using the encrypted wrapper and the keys for the devices. Ex-1004, [0026-0032].




Ex-1004, Fig. 1.

69. **Step 2A (adopted directly from Har as modified by Miller)**: This step checks if the content of the request matches the authentication server's data store.

> Moreover, <u>authentication server 102 can verify that information included in the transmission sent by the sender agrees with information for the sender stored in a data store associated with the authentication server 102</u>. If decryption is successful and the digital signature of the sender of the message is verified, <u>and the information included in the</u>

> transmission by the sender agrees with information stored in the data store of the authentication server 102…

Ex-1004, [0026].

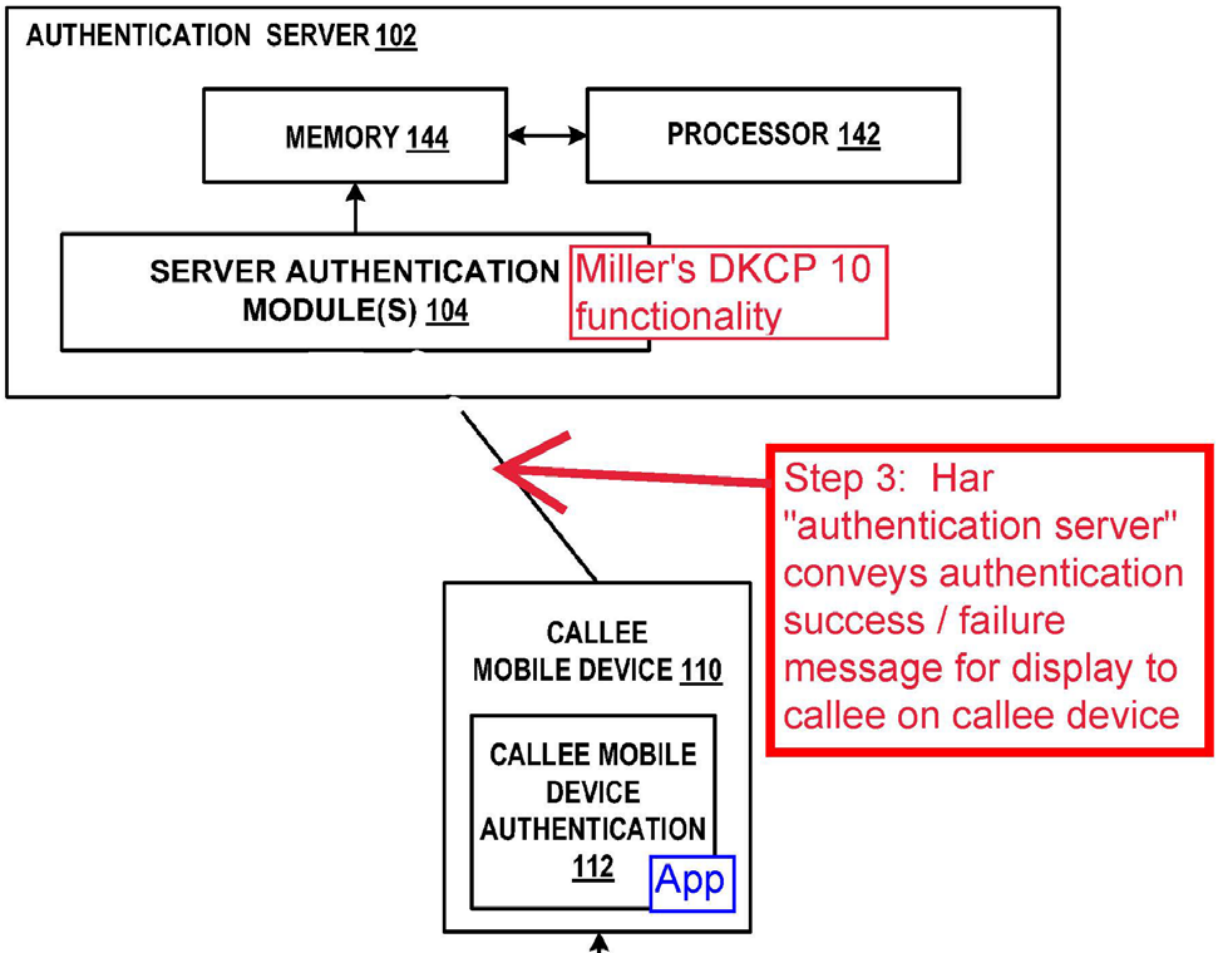
70. The emphasized sections above reflect Miller's augmented functionality included into Har. Miller's authentication processing includes computing a "score" based upon device minutia. Miller's score-based authentication process includes an optional iterative challenge / response sequence with the requesting / caller device to refine and improve the authentication process. *See* Section VII.A.2 (*supra*), elements 1.ii, 1.iii (*infra*). After the score is computed, the score is received by other components (including processors) for use in the security determination (e.g., comparing against thresholds) as detailed below for element 1.iii.(b).

71. Har's system includes a bi-directional "data channel" between the authentication server and mobile devices. Ex-1004, [0002-0003], [0031]. Har uses the "data channels" for the server, challenging the device for more authentication information and receiving a response with such authentication information. For example, in Har, users can be "prompted for credentials including but not limited to a password or personal identification number (PIN) code and/or other information." Ex-1004, [0019]. "The credentialing information can be verified against information

stored at the authentication server for the user." Ex-1004, [0019]; *see also* Ex-1004, [0029]. Thus, Miller's challenge / response interactions merely use an existing Har data channel for its normal and intended usage.

72. In the Har/Miller System, Har's "mobile device's" (106/108) are "smart phones" that both Har and Miller each identify. Ex-1004, [0001], [0045]; Ex-1022, [0048].

73. **Step 3 (adopted directly from Har)**: Har's authentication server conveys the success / failure of authentication to the callee's device for display to the callee. *See* element 1.v (*infra*); Ex-1004, [0028-0032].




Ex-1004, Fig. 1.

74. Separately, for registration with the authentication server, the Har/Miller System uses Miller's registration procedures (which Har also suggests) to store information about the users / devices in Har's authentication server. *See* Section VII.A.2 (*supra*), elements 1.iii, 1.iv (*infra*); Ex-1004, [0035] ("information associated with the first user, as registered in the server's database…").

75. Thus, the proposed Har/Miller System is merely Har's system with Miller's score-based authentication that bolsters Har's teaching of comparing information in the authentication request against information in the authentication server's data store for matches.

#### 4. Motivation to Combine the Teachings of Har and Miller

76. A POSA would have been motivated to combine Har with Miller to arrive at the Har/Miller System with a reasonable expectation of success.

77. The references themselves include motivations to combine. Har's authentication server performs a two-step authentication check (steps 2 and 2A above). Har emphasizes Step 2 (checking the digital certificate surrounding the authentication request). While Har teaches checking the authentication request's contents, Har does not detail how content of the request is matched to the authentication server's data store (step 2A above). Miller provides additional details, and additional security, to implement Har's step 2A.

78. Miller itself provides a motivation to augment Har for multiple reasons. First, a POSA would recognize that Miller's system provides significantly "increased security" and authentication for the reasons stated in Miller. Ex-1022, [0031-0033]. For example, Miller's system describes using a broad array of device

"minutia" which can be formed into different "subsets" for authentication. Ex-1022, [0031-0033]. By enhancing the authentication process and offering different forms of authentication bases (minutia), the Har/Miller System better effectuates Har's basic goal that the "authentication server can vouch for the identity of the [first/second] user, the message integrity and the message privacy." Ex-1004, [0002-0003]. Har identifies, and seeks to address, the problem of "security" when interacting with "service providers." Ex-1004, [0011-0013]. Miller's enhanced authentication provides "increased security" ([0031]) or "unprecedented security" ([0028] by using "dynamic" key information and by using the device-based unique identifiers (in various subsets) as increased protection against "spoofing" attacks when interacting with service providers. Ex-1022, [0028], [0011], [0033], [0041], [0045].

79. Miller details existing authentication systems including systems using "cryptographic keys" such as "symmetric, public or private" keys as are described in Miller. Ex-1022, [0006-0011]. Miller's "dynamic" system improves existing "static" key systems. Ex-1022, [0031-0033]. Miller describes an embodiment where the keys used to sign "digital certificates" (such as those described in Har) can be based upon Miller's dynamic key system for improved security. Ex-1022, [0133], [0047].

80. Thus, a POSA would have been motivated to augment Har's authentication functionality with Miller's DKCP functionality to improve security and better vouch for the calls and interactions with service providers as described in Har.

81. Moreover, a POSA would recognize that Miller's score-based system allows for significant flexibility by permitting interactions with the device being authenticated to "increase the scoring over the desired threshold" based upon using additional minutia information to verify the device. Ex-1022, [0104-0110]. The '989 patent later adopted this same flexibility of additional interactions between the authentication server and the device seeking to "raise the verification score" using other factors. Ex-1001, 9:55-10:20. Miller's scoring allows for a flexible "confidence scoring" and "confidence rating" which can use different "heuristics" to establish the authentication using many different forms of minutia – thus providing additional security and confidence in the authentication results as would be recognized as beneficial to a POSA. Ex-1022, [0103-0120].

82. Furthermore, by using Har's existing digital signature authentication wrapped around Miller's enhanced device-based authentication using scoring, a POSA would recognize benefits in overall system performance. For example, Har's system utilized existing, known techniques for the digital signatures. Thus, the

initial security determination (Step 2 above) can use known, existing technologies and algorithms for an initial check that can be performed efficiently and quickly. If the authentication using digital certificates fails using Har's "older" technology, then time and effort can be saved by not performing Miller's detailed additional authentication using Miller's scoring algorithm (Har's Step 2A above). This allows for efficiency through "quick fails" and requires only the more detailed processing (Step 2A) if the initial authentication (Step 2 using digital certificates) is successful. A POSA would recognize this as a performance benefit that retains the augmented security provided by Miller.

83. A POSA would be confident of the success of the modification as it is a software solution that uses known techniques – rules and logical arrangement of rules, and well-known cryptographic techniques and heuristic evaluation of multiple authentication factors – all for their intended purpose – implementing objectives of verifying a caller, including the validity of a phone number associated with the caller.

84. Har and Miller are also analogous art to each other, and to the claimed invention, being in the same field of authentication of communications and using information about the call, caller, and caller's device, to make a security determination about the treatment of a calls. Moreover, Miller provides details absent from Har regarding Har's system "that supports authentication of mobile

devices." Ex-1004, [0044]. Both Miller and Har are directed to the same problem as the '989 Patent – "[d]etermining the trustworthiness of information used to identify entities involved in communications" so the communication is not "spoofed by unscrupulous entities." Ex-1001, 1:27-31. *E.g.,* Ex-1004, [0002] ("authentication server can vouch for the identification of the first user, the message integrity and the message privacy."); Ex-1022, [0041] (DKCP "increases the difficulty of spoofing minutia values and intercepting calls intended to counterfeit the original computer").

85. Augmenting Har's *authentication* system to include Miller's DKCP authentication would be within a POSA's skill. Call authentication systems were well known in the art and combining the teachings of Har and Miller would involve routine skill to a POSA with a reasonable expectation of success. As detailed above, Har and Miller describe the same type of fundamental components (e.g., servers for authentication and smart phones for user devices being authenticated). Moreover, Har and Miller include bi-directional communication between the server and devices – including for the purpose of requesting and receiving additional authentication information. Thus, the basic architectures and data flows within Har and Miller are compatible and bolster a POSA's expectation of success.

.

### 5. Detailed Application of Har in view of Miller

#### a. Claim 1

i. A system, comprising:

86. If the preamble is limiting, Har and Miller disclose "systems." Ex-1004, [0020]; Ex-1022, Figs. 1-9.

ii. one or more processors configured to:

87. Har and Miller disclose systems comprising "one or more processors" configured to perform the actions below. Ex-1004, [0021], [0037], [0043]; Ex-1022, [0049]; [0015-0016], [0178-0185].

iii. receive information pertaining to a call initiated by a calling device, the information pertaining to the call including:

88. The Har/Miller system discloses this limitation and describes processor(s) configured to "receive information pertaining to a call" as detailed below. Moreover, as detailed below, the received information is "*pertaining to the call*" because it is received in response to the authentication process resulting from Har recognizing that a call has been initiated.

(a) (1) a value generated based at least in part on information associated with the calling device

89. The Har/Miller authentication server receives at least two distinct types of "*value[s] generated*" corresponding to this element: (1) Har's encrypted request with a digital signature; and (2) Miller's minutia (including computer minutia). All are used for authentication.

90. In the Har/Miller System, "[a] voice channel … connection can be initiated" and "an authentication process can be initiated" in which the caller "can send an authentication request, requesting the server to authenticate the identity of the first user" ("*receive information pertaining to a call…*") Ex-1004, [0014-0015].

91. **Har's received authentication request is encrypted and digitally signed using encryption keys.** Ex-1004, [0016]. Har's usage of encryption keys to encrypt and sign Har's authentication request is a "*value generated…*" because the keys correspond directly to the '989 specification portions identified by the applicant to the Examiner for this element.

The applicant amended the claims to recite:

> Receive information …including: (1) a [[code]] value generated based at least in part on information associated with the calling device…

Ex-1002, 0197. "Support for the amendments … may be found … in Paragraphs [0046] and [0048]-[0049]…." Ex-1002, 0195. Paragraph [0046] in the '989 application recites that the "*value generated*" may use a "key" that is "stored in a memory associated with the device" (and therefore "*based at least in part on information associated with the calling device*" according to the applicant):

> the verification processing resident on the device … generates a message based on a value stored in a memory associated with the device, … One example implementation is for the message to be a message authentication code on the phone number called, where the message authentication code is at least one of … an additional value that may be pseudo-randomly generated … using **a key that is stored on the device** ….

Ex-1002, 0041 (corresponding to Ex-1001, 8:31-52).

92. Har's "authentication request" with its encryption and digital signature disclose what the applicant told the Examiner was the claimed "*value*" (which corresponds to the authentication request as the encrypted message and/or the digital signature). Har's "device generates a message" using two "keys …stored on the device:" (1) the "server's public key" and (2) the "private key" stored in the device:

> The first user can send an authentication request, requesting the server to authenticate the identity of the first user …The authentication request can be a message encrypted using the server's public key (also called the server's public certificate) and signed using the private key (also called the private certificate) of the first user … using PKI authentication methodology (asymmetric key encryption/decryption). Alternatively, another type of authentication methodology can be used including but not limited to symmetric key encryption/decryption.

Ex-1004, [0016]; *see also* Ex-1004, [0023], [0018], [0025-0035] (all using keys for encryption and signature). Har's server "can decrypt the encrypted request using the server's public key and the digital signature can be verified using the public key of the user sending the message." Ex-1004, [0026], [0030].

93. Har's digital signature is a "value" generated using the caller's private key and teaches, or renders obvious, "*a value generated based at least in part on information associated with the calling device*." For example, the digital signature is a "value that may be pseudo-randomly generated, for example, using a key that is stored on the device" as cited to the Examiner from the '989 specification. Ex-1002, 0041, Ex-1001, 8:31-52. Similarly, Har's device uses the "server's public key" to encrypt the message. The overall encrypted message is a "*value generated*" based on the server's public key. Moreover, Har teaches the use of "symmetric" keys for

authentication which also corresponds to this value under the passages cited above to the Examiner.

94. Har's "private key" and "server's public key" are both "*associated with the calling device*" according to the applicant's statement to the Examiner because each is "a value stored in a memory associated with the device." Ex-1002, 0049, 0041; Ex-1001, 8:31-34. It would be obvious that Har's keys would be "stored in a memory associated with the device" in order to encrypt and digitally sign the authentication request. Har's "authentication server may have a data store of user information that includes the … public keys for users." Ex-1004, [0018]. Har's mobile device has a "memory" and a "cryptographic engine." Ex-1004, [0047-0048], Fig. 5. At a minimum, it would be obvious to store Har's keys used for encryption and signing in the device's memory for use by Har's cryptographic engine.

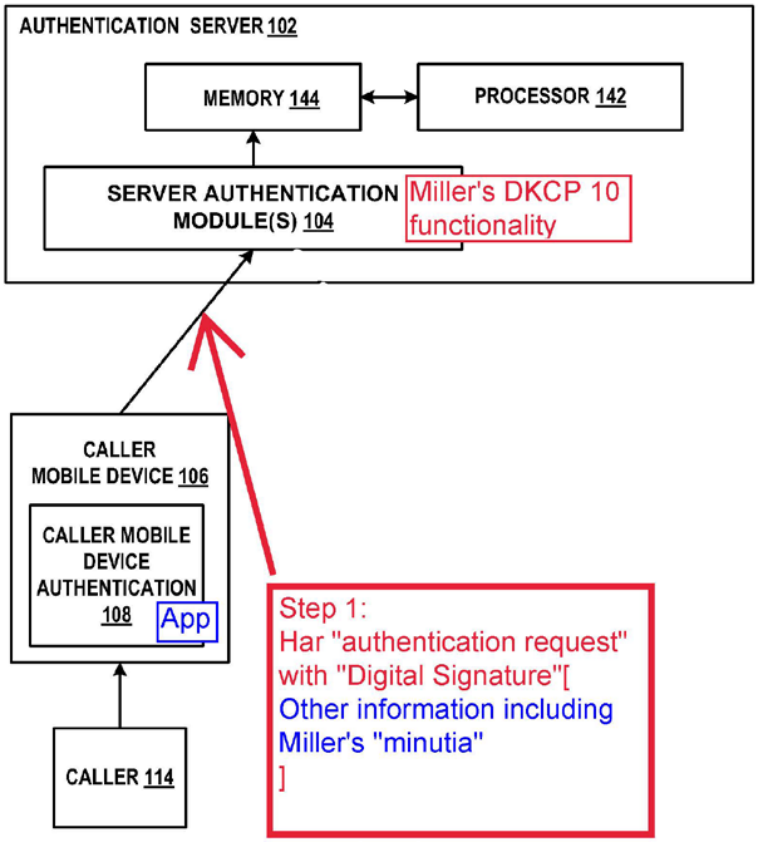
95. If PO argues that the claim is not met and that Har's "private key" is associated with a person and not the caller device, the Board should reject any such argument. First, it would be inconsistent with the applicant's statements to the Examiner (detailed above) and inconsistent with the '989 specification. Ex-1001, 8:2-3 ("value stored in a memory associated with the device"); 8:11-12.

96. Second, Har teaches, or renders obvious, that the "private key" is associated with the caller device. Har teaches that "FIG. 4 illustrates … a system 400 that supports authentication of mobile devices. … [with] an authentication server to authenticate mobile devices as described herein" which is a teaching that the authentication pertains to devices (not people). Similarly, Har uses the "server's public key" and "server's private key" to encrypt / sign messages. Ex-1004, [0016], [0018]. Har's server is a device (not a person) and thus, Har teaches such keys are associated with devices. Given these teachings, it would be an obvious variation to use a private key associated with the caller device to digitally sign the communication from the caller device to the authentication server. Such a usage would effectuate the goals of both Har and Miller to ensure correct authentication. Moreover, both Har and Miller provide storage on the caller device and authentication server of device-specific information used for authentication.

97. **Separately, Miller's authentication processing discloses this "*value generated*…" element**. Miller uses a variety of "minutia" including "computer minutia" for authentication. Miller can use "minutia" to generate a "hashed" *value* to reflect minutia combinations. Miller's "minutia" can be processed by a cryptographic function to generate a "key" *value*. Miller's minutia variants can be received by the authentication server both during a "registration" process and during

a request for authentication. As detailed below, each of these forms of minutia correspond to the claimed "*value generated*…"

98. As detailed in Section VII.A.3, the Har/Miller authentication request includes two pieces as detailed in Har: (1) the encryption / digital signature and (2) "other information" including Miller's minutia. Ex-1004, [0016], [0026].




Ex-1004, Fig. 1. As detailed in VII.A.3, Miller's minutia may also be received by a challenge/response sequence between the server and device. E.g., Ex-1022, [0039].

99. Miller's DKCP receives "[i]dentification based on a hash from a subset of minutia taken from a very wide range of minutia found or collected by the computer including hardware, firmware, software, user secrets, and user biometrics" Ex-1022, [0039]; *see also* Ex-1022, [0050-0060] (detailing various minutia); Fig. 2 (elements 2001, 2003, 2005, 2007, 26) (showing different minutia). Miller's "computer minutia" (hardware, software, firmware minutia) is specifically associated with computer 18 (calling device). Ex-1022, [0031], [0039], [0052-0053]. Miller's DKCP may identify and receive minutia subsets for authentication. Ex-1022, [0061]; Figs. 2A-2B. Miller creates a unique device identifier using sets of "computer minutia" to provide "unique identification" of devices. Ex-1022, [0050]; *see also* Ex-1022, [0056].

100. Miller's "hash from a subset of minutia" is a "*value generated based at least in part on information associated with the calling device*." Ex-1022, [0039], [0051], [0094], [0011]. Miller's "hash" is "often referred to as a computer fingerprint." Ex-1022, [0011], [0038-0039], [0051], [0094], [0132-0133], [0142-0143]. For example, Miller may use a "combination of minutia [of] one hardware minutia, Hx, one firmware minutia, Fy, and one software minutia Sz." Ex-1022, [0057]. This "tripley Hx-Fy-Sz" may be represented by a single number and "any combination of minutia … may be used." Ex-1022, [0057-0060]. Miller gives an

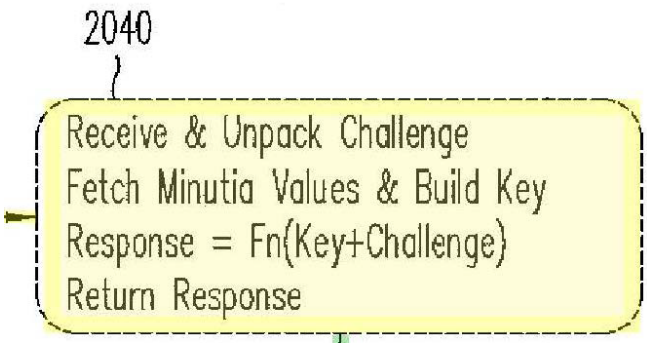
exemplary generated hash value of "Resp 172" to represent a pre-processed hash of a particular combination of minutia. Ex-1022, [0066]. This pre-processed hash is a "*value generated…*" as claimed because it is generated based on the specific minutia (including the computer minutia) that is associated with a calling device (and seeks to uniquely identify that device).

101. Miller's "key" generated by using the minutia and an "cryptography function" is also a "*value generated based at least in part on information associated with the calling device*." Miller uses minutia (either hashed or unhashed) to generate a "key" that is received by Miller's authentication server. Ex-1022, [0060-0066].

Miller's device will:

> At step 2040 … fetch the values of the selected computer minutia 64 …and build a key that may be identical to the key computed by the dynamic key crypto provider 10 at step 2020. The particular computer 18 being challenged may form a response to the challenge by applying a mathematical or cryptographic function "Fn", which should be the same as that used at step 2020 or step 2030, to the key+challenge as shown in FIG. 2. The computer 18 being challenged may then communicate the response to return it directly to the dynamic key crypto provider 10 …

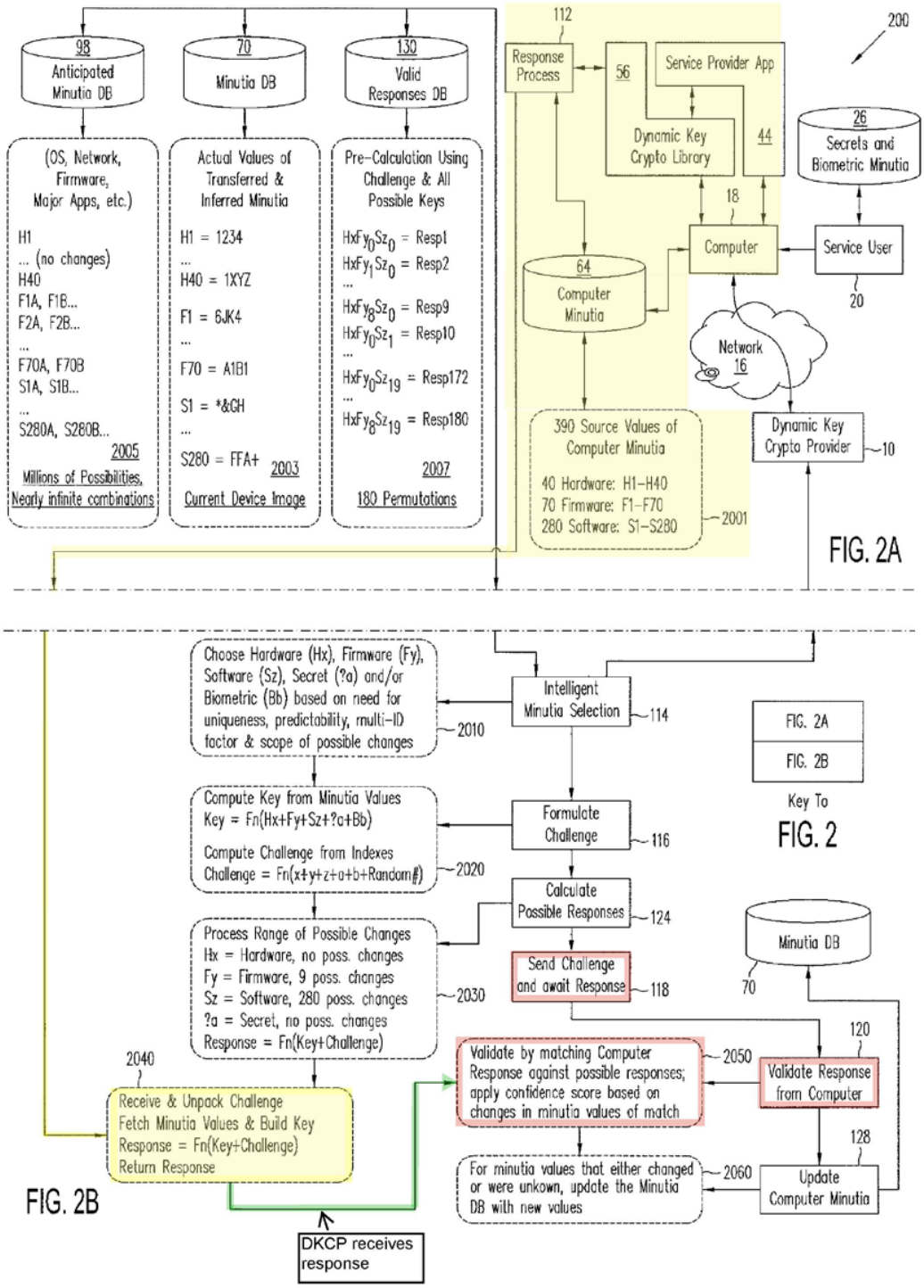
Ex-1022, [0065]. Element 2040 in Miller's Fig. 2 depicts creating and returning the response to the server:




Ex-1022, Fig. 2B; See also Ex-1022, [0063] (describing "step 2020" which "compute[s] a cryptographic key based on the selected combination of minutia …."), [0013-0016], [0080] ("digital signature").

102. Thus, Miller's authentication information shows "*a value generated based at least in part on information associated with the calling device*" in three separate examples: (1) minutia in unhashed form; (2) minutia in hashed form; and/or (3) the "key" which is built by the "cryptographic function 'Fn'" applied to either the hashed or unhashed versions of the minutia.

103. Thus, the Har/Miller system discloses this element in multiple distinct examples. Miller's Fig. 2 depicts Miller's challenge / response process of the DKCP receiving various values from the device.


98
Anticipated Minutia DB
70
Minutia DB
130
Valid Responses DB
(OS, Network, Firmware, Major Apps, etc.)
H1
... (no changes)
H40
F1A, F1B...
F2A, F2B...
...
F70A, F70B
S1A, S1B...
...
S280A, S280B...
2005
Millions of Possibilities, Nearly infinite combinations
Actual Values of Transferred & Inferred Minutia
H1 = 1234
...
H40 = 1XYZ
F1 = 6JK4
...
F70 = A1B1
S1 = *&GH
...
S280 = FFA+
2003
Current Device Image
Pre-Calculation Using Challenge & All Possible Keys
HxFy0Sz0 = Resp1
HxFy1Sz0 = Resp2
...
HxFy8Sz0 = Resp9
HxFy0Sz1 = Resp10
...
HxFy0Sz19 = Resp172
...
HxFy8Sz19 = Resp180
2007
180 Permutations
112
Response Process
56
Service Provider App
Dynamic Key Crypto Library
44
200
26
Secrets and Biometric Minutia
18
Computer
Service User
20
64
Computer Minutia
Network 16
390 Source Values of Computer Minutia
40 Hardware: H1–H40
70 Firmware: F1–F70
280 Software: S1–S280
2001
Dynamic Key Crypto Provider
10
FIG. 2A
Choose Hardware (Hx), Firmware (Fy), Software (Sz), Secret (?a) and/or Biometric (Bb) based on need for uniqueness, predictability, multi-ID factor & scope of possible changes
2010
Intelligent Minutia Selection
114
FIG. 2A
FIG. 2B
Key To
FIG. 2
Compute Key from Minutia Values
Key = Fn(Hx+Fy+Sz+?a+Bb)
Compute Challenge from Indexes
Challenge = Fn(x+y+z+a+b+Random#)
2020
Formulate Challenge
116
Calculate Possible Responses
124
Process Range of Possible Changes
Hx = Hardware, no poss. changes
Fy = Firmware, 9 poss. changes
Sz = Software, 280 poss. changes
?a = Secret, no poss. changes
Response = Fn(Key+Challenge)
2030
Send Challenge and await Response
118
Minutia DB
70
120
2040
Validate by matching Computer Response against possible responses; apply confidence score based on changes in minutia values of match
2050
Validate Response from Computer
Receive & Unpack Challenge
Fetch Minutia Values & Build Key
Response = Fn(Key+Challenge)
Return Response
128
For minutia values that either changed or were unkown, update the Minutia DB with new values
2060
Update Computer Minutia
FIG. 2B
DKCP receives response

The "computer 18" components and algorithm are highlighted in yellow. The DKCP uses that "response" to validate the computer as highlighted by boxes 118, 120, 2050.

(b) (2) a score generated for the calling device, the score indicating a validity of a phone number

104. The Har/Miller System teaches this "score." in two ways: (1) Miller's "score" computation; and (2) Miller's use of "user biometrics."

105. First, Miller "computes" a "score" based upon the "minutia" discussed in element 1.iii.(a) (*score generated for the calling device…*). Fig. 6A shows the "compute score 144" functionality:

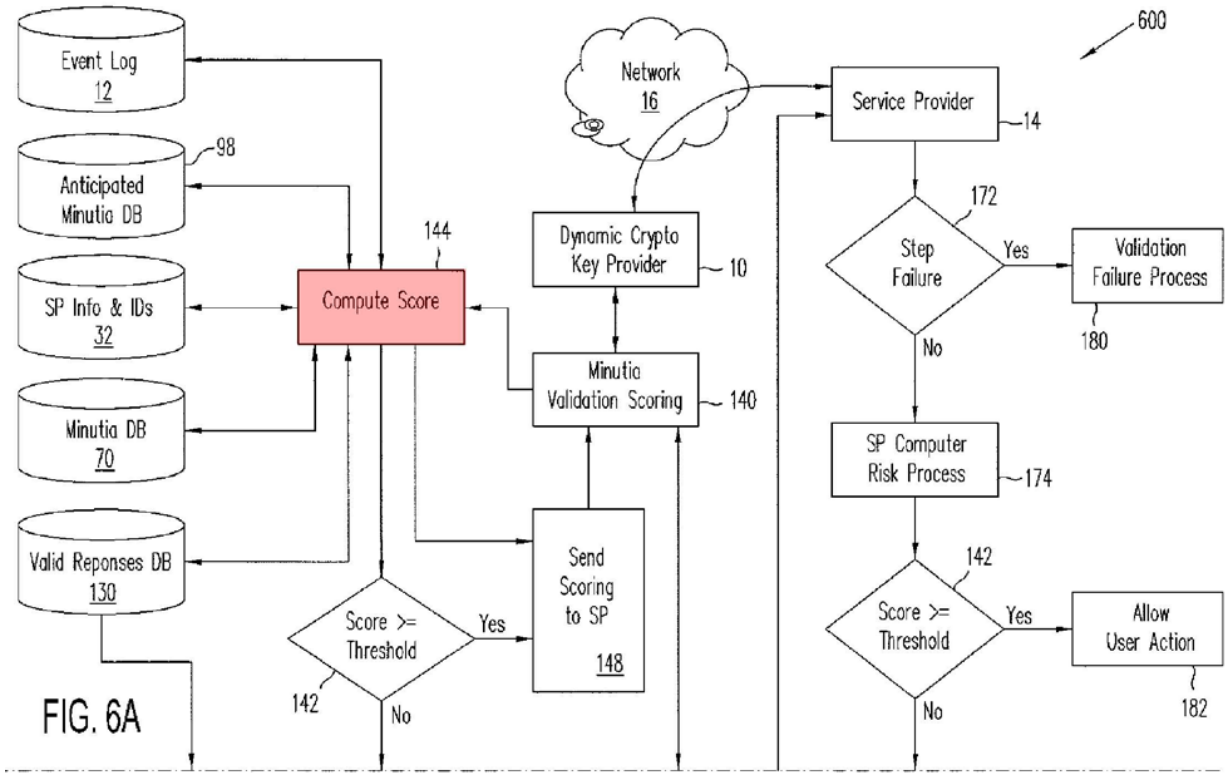



FIG. 6A

Ex-1022, Fig. 6A. Miller' "scoring" matches received minutia (optionally hashed or encrypted) against stored minutia information to validate the authentication request. Ex-1021, [0040] ("[s]coring the confidence of a valid response based on the minutia"); [0073], [0100], [0102-0120]. Miller's scoring uses a "vast number of minutia to be validated." Ex-1021, [0106-0109].

106. Miller's "*score indicating a validity of a phone number*" mirrors the passages cited by the applicant to the Examiner. When the applicant added the "score" element during prosecution, the applicant cited to "Paragraphs [0046] and [0048]-[0049]" in the application. Ex-1002, 0195, 0197. "Paragraphs [0048]-

[0049]" in the '989 application teach "a score indicating the validity of the number" ([0048]) and that "the verification score is created using a variety of approaches that include one or more of combining the available factors to create a score by applying relative weighting to each of the available factors" ([0049]). Ex-1002, 0041, 0043 (corresponding to Ex-1001, 9:1, 9:38-45). Thus, "*a score indicating a validity of a phone number…*" encompasses combining various information ("available factors") about the call / communication and the related devices to calculate the score. Ex-1001, 9:20-57. In the '989 patent (as in Miller) the authentication server may request additional information to the calling device in an attempt to raise the score. Ex-1001, 9:34-10:20.

107. Miller generates a "score" by combining available factors, including minutia, as described in the '989 patent (and cited to the Examiner):

> [C]ompute score 144 process computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response using data from the valid responses DB 130, the SP info and IDs 32 data, the event log 12 and the anticipated minutia DB 98. …

Ex-1021, [0105]; [0103]. Thus, Miller's "score" discloses a "*score generated for the calling device, the score indicating a validity of a phone number*" for the same reasons as the "score" cited to the Examiner.

108. Miller's "*score indicat[e]s a validity of a phone number*" for further reasons. In the context of the Har/Miller System, authentication is performed for the "authentication request" associated with the call using the caller's identification to "vouch for" the caller. Ex-1004, [0002]. This teaches, or renders obvious, that the score relates to the validity of the caller's phone number because, at a minimum, the caller's device phone number is one form of identification. Ex-1004, [0018]. It is also obvious that, when authenticating a voice phone call (as in Har), the authentication encompasses indicating the validity of the phone number(s) of devices engaged in that call.

109. Furthermore, the Har/Miller system may use the phone number as one minutia ("available factor") to generate the score. As detailed in 1.iii.(a), Har receives and uses in its authentication server both the identity/identification of the caller, when renders teaches or renders obvious the caller's phone number. Ex-1004, [0002], [0016]. Similarly, Miller's "collection of minutia" includes "phone numbers." Ex-1022, [0051]; *see also* Ex-1022, [0067] (a "validate response … can employ multiple methods of collecting … a smartphone's phone number" or a "phone number" in the "returned minutia."). Thus, the Har/Miller system can receive, store and utilize the phone numbers of registered users (including callers) for scoring validity of a call.

110. Thus, in the context of the Har/Miller authentication server, because the focus of the system is security verification within the context of telephone calls, it would be obvious to use the phone number associated with the caller device or callee device as one minutia within Miller's scoring system. Moreover, Miller describes an iterative challenge/response process increase the score. Ex-1022, [0067], [0104], [0113-0120], [0045]. Furthermore, "Different minutia can be intelligently chosen …to …yield[] a higher confidence score, … and particular minutia isolation." Ex-1022, [0040]. In one exemplary usage of Har/Miller, the scoring would assess the phone number minutia either as part of the initial scoring or as part of subsequent attempts to increase the score to reflect the validity of the phone number ("particular minutia isolation" as quoted above).

111. Thus, given the overlap between the "scoring" in Miller and the '989 patent, the Har/Miller scoring system at a minimum renders obvious that the computed score "*indicat[e]s a validity of a phone number*."

112. **Miller also teaches "*one or more processors configured to receive … a score generated …*."** for the computed score. As shown below, Miller teaches at least eight separate "software components" (Ex-1022, [0184]) that receive Miller's computed score (elements 142, 148, 150, 152, 154 156, 158, 160) ("Receiving

Components") as indicated by the yellow boxes and red arrows in Figs. 6A/6B below:

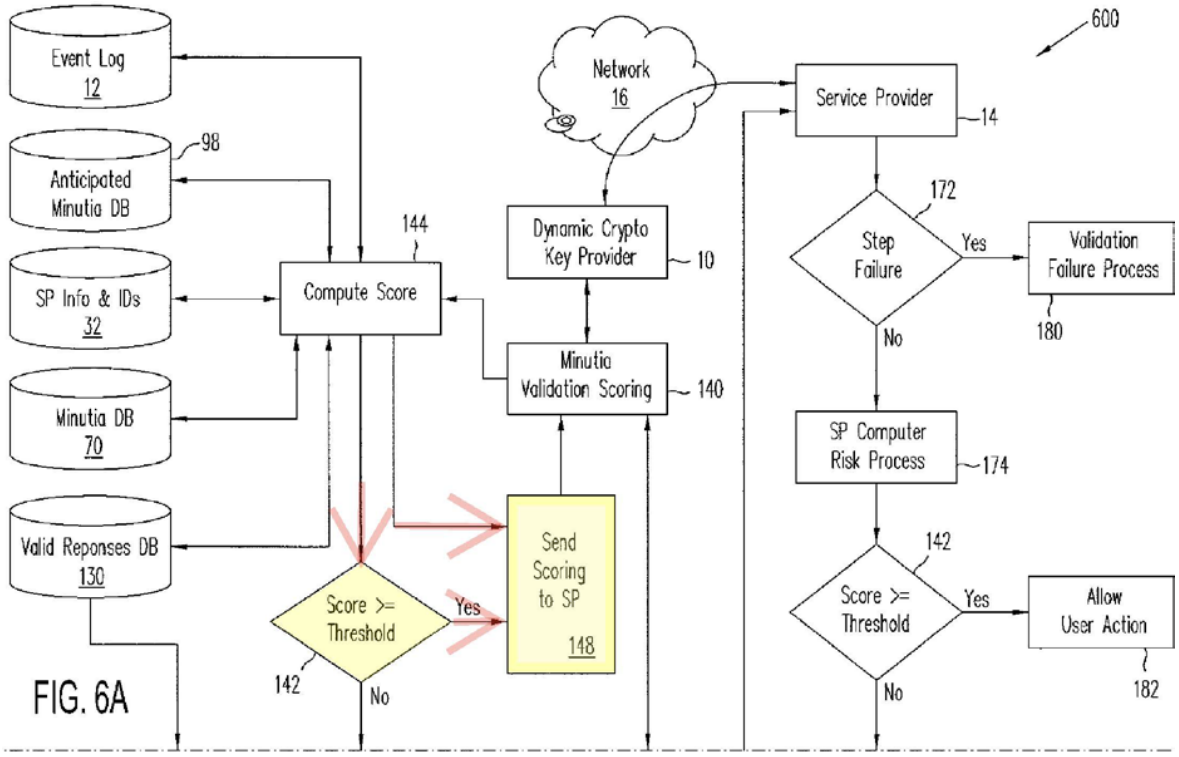
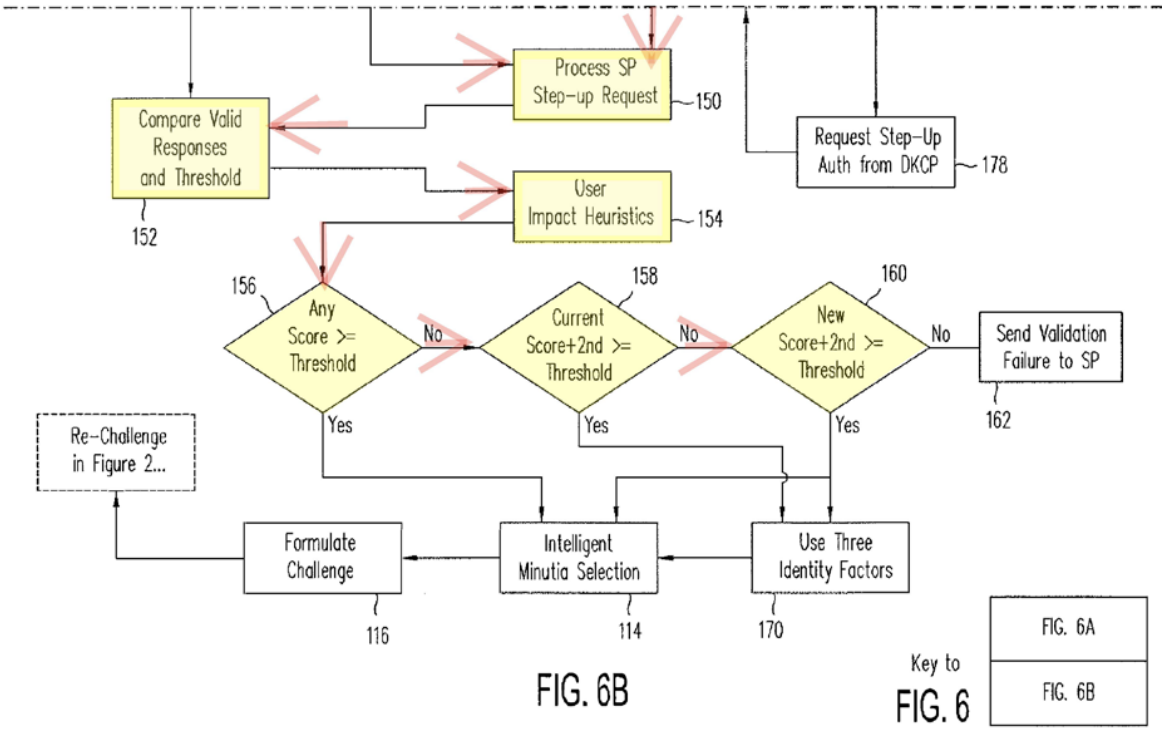



FIG. 6A




Ex-1022, Figs. 6A/6B; [0111-0120] (describing the Receiving Components using the score). Miller's actions can be performed by software executing on one <u>or more</u> processors. Ex-1022, [0177-0185]. Thus, use of the computed "score" teaches, or renders obvious, that the score was "received" by the processor executing the software implementing the Receiving Components after the score was computed.

113. Using Miller's teachings, the "processor" that receives the scores can be either: (1) the same processor computing the score or (2) a processor different from the one computing the score. Miller teaches that its processing can be distributed across different hardware components (processors):

> the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both ….

Ex-1022, [0184]. Similarly, Har's authentication server (implementing Miller's DKCP functionality) can performed its functionality by one or more processors. Ex-1004, [0021] ("Authentication server 102 can include a processor (such as processor 142) ….. Authentication server 102 can include one or more modules comprising one or more authentication modules, represented in FIG. 1 by server authentication module 104. … the above described module or modules can be loaded into memory 144 to cause one or more processors … to perform the actions attributed to the modules").

114. The '989 patent matches Miller's distributed system with "sub-components" (processors) performing different aspects of the verification.:

> Verification service provider 120 can also be implemented using a scalable, elastic architecture and may comprise several distributed components, including components provided by one or more third parties. Further, when verification service provider 120 is referred to herein as performing a task, such as storing data or processing data, it is to be understood that a sub-component or multiple sub-components of verification service provider 120 (whether individually or in

> cooperation with third party components) may cooperate to perform that task.

Ex-1001, 4:14-23. Thus, Miller's embodiment in which a different processor "receives" the computed score for subsequent evaluation corresponds directly to one of the '989 patent embodiments.

115. At a minimum, given that Har, Miller, and the '989 patent all describe embodiments in which multiple processors may perform the functionality of their authentication servers (as detailed above), the Har/Miller System discloses, or it is at least obvious, and an obvious implementation, that a separate processor would "receive" the "score" after it has been computed as detailed above and meets this element.

116. Second, Miller's DKCP *receives* "user biometrics minutia" from the device which a POSA would understand to teach, or render obvious, a "score." Ex-1022, [0028], [0131-0133], [0172-0174]. Miller's minutia includes "biometric information … collect[ed] from the user (e.g., fingerprint, voiceprint, [] retinal scan)" or "facial geometry." Ex-1022, [0031], [0054]. It would be obvious to a POSA that the collection / usage of such biometrics involves generating a "score" to reduce these characteristics to values usable in computers. Ex-1022, [0022], [0031-

0043] (describing calculating "scores" for "biometrics … (e.g., voice, fingerprint, iris, physical appearance…)").

iv. perform a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device; and

117. The Har/Miller system performs the claimed security determination in multiple different fashions. First, Har teaches that both the digital certificate authentication and authentication using the information within the request may be used as a security determination.

> An authentication server such as authentication server 102 can receive the authentication request, can decrypt the encrypted request using the server's public key and the digital signature can be verified using the public key of the user sending the message. … Moreover, authentication server 102 can verify that information included in the transmission sent by the sender agrees with information for the sender stored in a data store associated with the authentication server 102. If decryption is successful and the digital signature of the sender of the message is verified, and the information included in the transmission by the sender agrees with information stored in the data store of the authentication server 102, the transmission (the identity) of the sender is authenticated.

Ex-1004, [0026]. This teaches the claimed "*security determination based at least in part on*:" (1) the certificate-based determination (*verifying the value included in the information pertaining to the call initiated by the calling device*); and (2) the "information included in the transmission sent by the sender" (corresponding to Miller's score discussed below and in 1.iii.(b)) (*the score generated for the calling device*).

118. As detailed for element 1.iii.(b), Miller's "scoring" teaches, or renders obvious, a "*security determination based at least in part on the score generated for the calling device*." After Miller's score is generated / computed, it is evaluated against various "thresholds" to raise the score through additional authentication and/or determine the success or failure of the authentication ("*perform a security determination*…"). Ex-1022, Figs. 6A/6B (shown above), [00111-0120].

119. Miller's "threshold" comparison matches the '989 patent claim 25 (*infra*). The '989 patent claim 25 was prosecution claim 30 and "[s]upport for new claim 30 may be found… in Paragraph [0051] of the Specification." Ex-1002, 0389, 0392. "Paragraph [0051]" corresponds to Ex-1001, 10:6-20 and mentions, at most, a "score … is too low" and a process to "raise the verification score" based on additional authentication requests between the server and device. Ex-1002, 0043,

Ex-1001, 10:6:20. Thus, Miller's "threshold" evaluation corresponds directly to the score-based security determination identified by the applicant to the Examiner.

120. Similarly, Miller's "biometric" minutia matching reflects a score-based security determination as detailed in 1.iii.(b). It would be obvious to a POSA that "matching" such biometrics includes comparing the device biometric score against a "threshold" score. Ex-1022, [0031]; *See* Ex-1024, [0029], [0036].

121. Har's authentication server evaluation of the encryption and digital signatures corresponds to a "security determination … at least in part by verifying the value included in the information pertaining to the call initiated by the calling device." "If decryption is successful and the digital signature of the sender of the message is verified" (by using the various keys), "the transmission (the identity) of the sender is authenticated." Ex-1004, [0026]. See also Ex-1004, [0017], [0030] (describing the server successfully decrypting and verifying the authentication request and digital signature).

122. Har's encryption / signature key embodiment matches the '989 patent claims 3 and 4 (infra). During prosecution, the applicant told the Examiner that "support" for these claims was in "Paragraphs [0046] and [0065] of the Specification." Ex-1002, 0147 (corresponding to Ex-1001, 8:31-54, 12:32-53). These passages do not recite "security determination" but do recite the "key is used

to validate the device…" Ex-1001, 12:52-53. Such "validation" using the "key" is exactly what Har's encryption / digital signature teaches. Thus, Har teaches exactly what the applicant cited in the '989 patent as a "security determination."

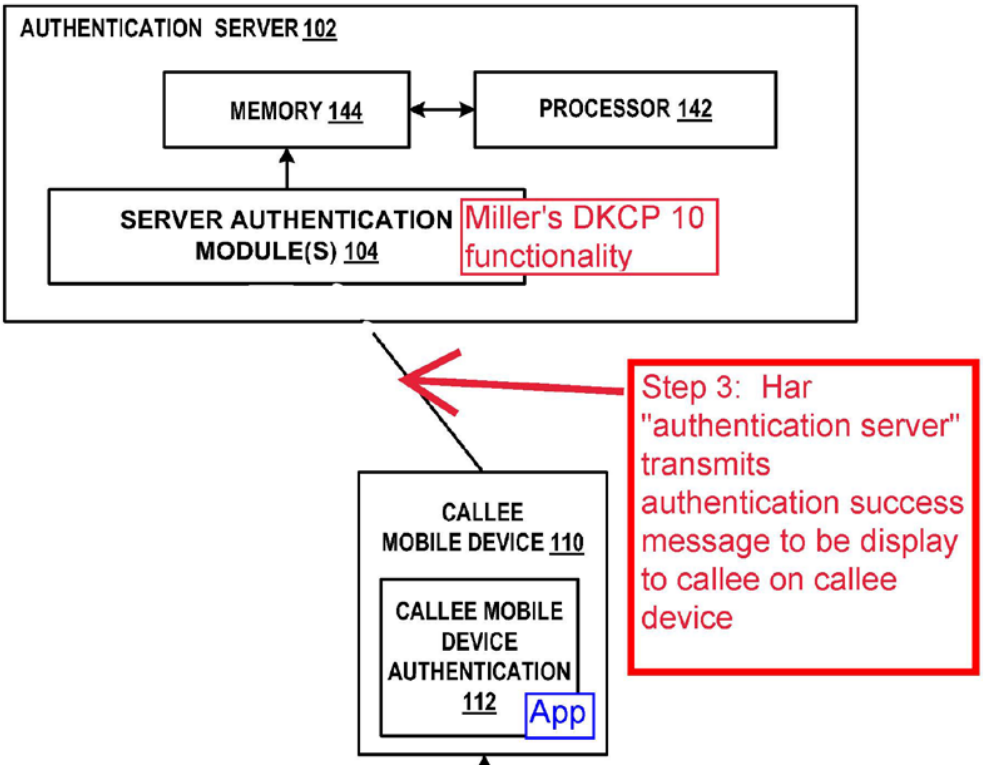
123. Similarly, as identified in element 1.iii.(a), Miller's process of comparing ("matching") minutia in an authentication request against stored minutia corresponds to "*security determination ... at least in part by verifying the value included in the information pertaining to the call initiated by the calling device*." Ex-1022, [0050] ("the validate response from computer 120 process can therefore be determined by simply comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match."); [0070], Abstract; [0014-0016], [0056], [0091].

124. Thus, the Har/Miller System teaches this claimed security determination.

v. based at least in part on the security determination, perform at least one of conveying an assurance to a callee associated with the call or conveying a

failure to confirm to the callee associated with the call; and

125. The Har/Miller authentication server conveys an assurance to the callee devices that may be displayed to the callee person. This assurance was explained in Section VII.A.3 as "Step 3" (incorporated herein):




Ex-1004, Fig. 1.

126. Har's server transmits a message to the callee indicating the security determination results (*convey[s] an assurance…*). "A message indicating success or failure of authentication can be prepared and sent to the second user…." Ex-1004,

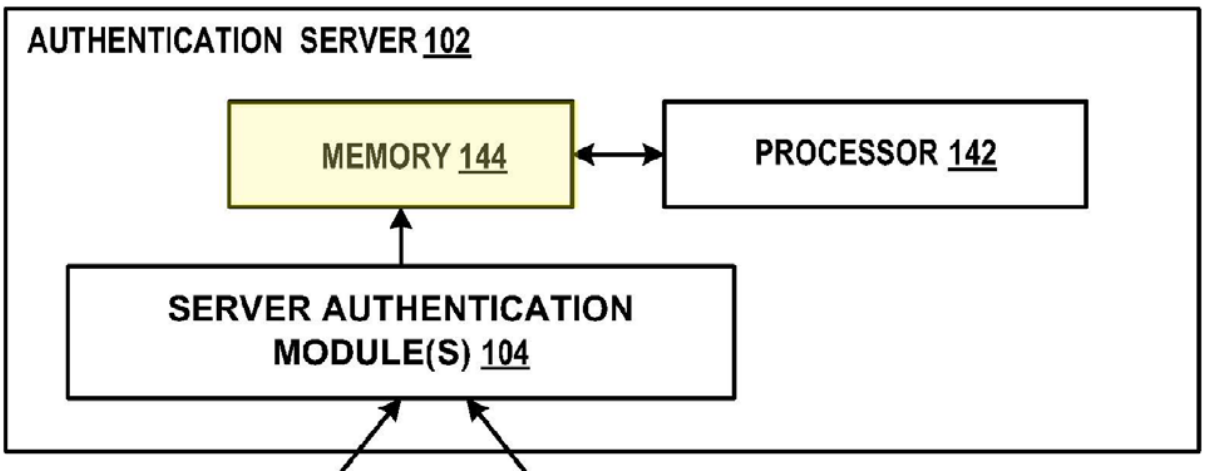
[0018]; *see also* Ex-1004, [0002], [0017-0018], [0026-0027], [0030-0035] (success message based on authentication); [0017] (authentication failure message).

127. Miller also discloses such conveying of assurance and failure. *E.g.*, Ex-1022, [0111], [0068], [0117] (each sending either the score or failure to the call recipient).

128. Thus, Har expressly teaches the element upon which patentability was based. Section V.B, *supra*.

vi. a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

129. The Har/Miller authentication server contains this element. Har discloses this limitation.



Ex-1004, Fig. 1, [0021] ("modules can be loaded into memory 144 to cause one or more processors such as processor 142 to perform the actions attributed to the modules…"), Fig.1. Miller discloses this limitation. Ex-1022, [0178-0184].

**b. Claim 2**

> The system recited in claim 1 wherein the information associated with the calling device is stored at an entity external to the calling device.

130. The Har/Miller System discloses this claim in the information stored at the authentication server (and at the device). *See* 1.iii.(a). Such dual-storage at the authentication server corresponds to the passages cited by the applicant to the Examiner for this claims.

131. Claim 2 was prosecution claim 3. Ex-1002, 0144. "Support for new Claim 3… may be found … in Paragraphs [0046] and [0065] of the Specification." Ex-1002, 0147. "Paragraphs [0046] and [0065]" correspond to Ex-1001, 8:31-54, 12:32-53. Ex-1002, 0041, 0047. Each of "Paragraphs [0046] and [0065]" describe that the device and the "verification service" server can each store duplicate copies of the same "information." E.g., Ex-1002, 0041 ("a key that is stored on the device and <u>also stored in a memory associated with the verification service provider</u>"), 0047

("the user device stores the derived or generated secret key, and a storage associated with the verification service also stores the secret key."

132. Har and Miller disclose such dual-storage of information at the device and authentication server. For example, Har teaches that its "keys" used for each of encryption and digital signature can be "symmetric" keys. E.g., Ex-1004, [0016] ("another type of authentication methodology can be used including but not limited to symmetric key encryption/decryption"); [0021], [0026-0032], claim 6. In such "symmetric keys," the same keys (used for encryption and/or signing) are stored on both ends of the communication (*e.g.,* device and authentication server). Thus, Har teaches exactly what the applicant told the Examiner corresponds to this claim (the same keys stored on the device and server).

133. Similarly, as detailed in 1.iii.(a) and 1.iv, Miller's minutia is stored on both the device and the server in unhashed form, in hashed form, or encrypted – which all correspond to present claim 2 – to be able to compare during the verification / authentication process. In particular, Miller's encrypted "key" stores the same "key" on both the device and the server as part of its authentication process. Thus, Miller also directly teaches exactly what the applicant told the Examiner corresponded to claim 2.

**c. Claim 3**

> The system recited in claim 1 wherein the information associated with the calling device comprises a cryptographic key associated with the calling device.

134. Har and Miller each disclose the cryptographic key as detailed in element 1.iii.(a). Har's encrypted signature sent to the authentication server is generated based upon the callee's private key (*cryptographic key associated with the calling device*). Ex-1004, [0016], [0023], [0025]. Miller's caller device calculates a "key" using a "cryptographic function" (*cryptographic key associated with the calling device*) as explained in 1.iii.(a).

**d. Claim 4**

> The system recited in claim 1 wherein the value is generated based at least in part on one of symmetric key cryptography and asymmetric key cryptography.

135. The Har/Miller system discloses this limitation for the same reasons discussed with respect to Claims 1.iii.(a) and 3. Har uses "asymmetric or symmetric key encryption/decryption methodologies." Ex-1004, claim 6, [0016]. Miller's key is *symmetric* because both the device and server use the same (computed) key for successful decryption.

**e. Claim 5**

> The system recited in claim 1 wherein the score for the calling device is generated in response to the call being initiated by the calling device.

136. The Har/Miller System generates a score to authenticate the caller when the device initiates a call and seeks authentication through the authentication request and process occurring in response to the initiation of that call. Claim 1.iii.

**f. Claim 6**

> The system recited in claim 1, wherein the score for the calling device is generated based at least in part on information associated with a user that is associated with the calling device.

137. Miller discloses that its "minutia" used for computing the "score" can optionally include "user secrets, and user biometrics" which are the claimed "information…." Ex-1022, [0012], [0031], [0042-0045], [0067]; element 1.iii.(b) (detailing scoring). Moreover, the "compute score" function "us[es] data from the valid responses DB 130, the SP info and IDs 32 data, the event log 12 and the anticipated minutia DB 98." Ex-1022, [0105]. "The SP info and IDs 32 database may be, for example, a list of customers…." The "anticipated minutia DB 98" includes the minutia such as user "secrets" and "biometrics of" the caller. Ex-1022,

[0056], [0173], [0067]. These are all "*information associated with a user that is associated with the calling device*."

**g. Claim 7**

> The system recited in claim 1 wherein the information pertaining to the call further includes at least one of a timestamp associated with the call and a called phone number.

138. The Har/Miller System discloses, or renders obvious, each of "t*imestamp associated with the call and a called phone number*." The Har/Miller authentication server teaches, or renders obvious, receiving "*a called phone number*" in multiple ways. Har's "request" includes "information identifying the callee." Ex-1004, [0023]; *see also* Ex-1004, [0016]. Furthermore, Har's authentication server "*receives*" data for its data store:

> The authentication server may have a data store of user information that includes the <u>mobile telephone numbers of users</u>, …, credentialing information, <u>identification information</u> and so on.

Ex-1004, [0018]. This disclosure shows two forms of "*a called phone number*." First, because Har's authentication request included "information identifying the callee" (Ex-1004, [0023]) it would be, at a minimum, obvious that such "information identifying the callee" corresponds to "user information" which includes the callee's

phone number ( "*a called phone number*"). It is also obvious that the "authentication request" would include the phone number so that the authentication server could identify the called device and communicate with it. Furthermore, it is also obvious, and well-known, that information related to a call includes the called phone number.

139. Second, Har's authentication server "can look up the mobile telephone number of the second user in its data store." Ex-1004, [0027]; [0018]. To "look up" this number in a "data store", it is at least obvious that the authentication server "received" the callee user's phone number at some point – such as through a registration process for the users. Ex-1004, [0035] ("information associated with the first user, as registered in the server's database"). This is "*information pertaining to a call*" because it allows the authentication server to contact the called device, such as for a PIN verification.

140. Furthermore, Miller's DKCP functionality includes the functionality to receive, store and utilize "*a called phone number.*" The "collection of minutia" includes "phone numbers." Ex-1022, [0051]; *see also* Ex-1022, [0067], [0052], [0056]; [0085-0094] (registration). Miller's DKCP communicates with the callee device ("service provider"). Ex-1022, Figs. 1, 4, [0085-0089]. In the context of Har's disclosure focused on mobile phones, it would be at least obvious that the

authentication server would have received the called phone number to communicate with the recipient device.

141. Thus, it would be at least obvious that the Har/Miller authentication server would receive "*a called phone number*."

142. Miller also discloses, or renders obvious, "*a timestamp associated with the call*." In Miller's security determination:

> [a]nother **scoring** input can be the time since a particular minutia value was last validated in a challenge and response exchange with the computer 18.

Ex-1022, [0109]. Miller's usage of the timestamp as a "scoring" input matches the '989 patent:

> the message sent to the verification service includes a timestamp, which can be used to prevent a replay attack. For example, the timestamp can be used by the verification service to **score** the validity of the communication, where an old or aged timestamp may be indicative of an attack.

Ex-1001, 8:58-63.

143. In Miller, to use (or calculate) the "time since a particular minutia value" in a request was last validated, it would be obvious (at a minimum) that the DKCP would beneficially know the timestamp of the current request being scored.

At a minimum, this "time since…" language renders obvious the use of a timestamp of the current communication being scored because a timestamp provides one input (the current time) to be compared against another input (the previous time the minutia was validated) for evaluating the "time since" aspect. Consistent with this evaluation, Miller describes how the other input (the minutia validation time) is collected and stored for usage. For example, Miller teaches that the "current device image" (used for the security determination / validation) is associated with collecting information "at a particular time or within some pre-defined time frame" and used for verification. Ex-1022, [0055-0056], claim 29. Miller identifies "time and time zone" as minutia used for verification. Ex-1022, [0067]. Miller uses these time-based verifications to prevent attacks that "intercept" and seek to use later "fraudulent responses" based on the interception. Ex-1022, [0029], [0067], [0041], [0135].

144. Miller's additional authentication process prompts a user for a "PIN." Ex-1022, Fig. 7, [0121-0133]. The "PIN" entry includes determining the "time since last successful PIN entry." Ex-1022, [0129]. Using this "time since" also requires usage of the current request timestamp to perform the comparison (for the same reason as detailed above).

145. Miller also describes a "heartbeat" process using a timestamp associated with the call for a security determination and that a response must be provided "within a timeframe" or otherwise the service is deleted. Ex-1022, [0150-0151]. To determine that the response message was "within a timeframe," it would be (at a minimum) obvious that the response included a timestamp to use as one of the inputs to this determination.

146. Furthermore, Miller describes its system as providing a "digital signature." Ex-1022, [0132-0133]. Using this "digital signature" aspect of Miller's DKCP system, "the dynamic crypto key can bind the instrument, place, time and person to a particular message." Ex-1022, [0133]. This teaches, or renders obvious, that the "key" generated by the computer 18 includes a timestamp associated with the communication and is used for the security determination (as detailed in 1.iii). Finally, Miller notes that it was already known in the art to perform verification / identification through "analysis of time (both in clock and network latency)." Ex-1022, [0011].

147. Moreover, Har's usage of public/private keys (certificates) as detailed in 1.ii and 1.iii also renders obvious the use of a timestamp as detailed in this claim. A POSA would understand that such public / private keys typically have an expiration time associated with the key. It would be obvious that the evaluation of

such keys would include a comparison of the timestamp of the current communication against the expiration time of the key used for the authentication.

**h. Claim 8**

> The system recited in claim 1 wherein the security determination is performed by one of a device associated with a called phone number and an entity different from the device associated with a called phone number.

148. This claim does not have meaning because it recites an action (*security determination*) to be *performed* anywhere (by the "*device*" or "*an entity different from the device*."). The Har/Miller System performs the claimed *security determination* at the "authentication server" which is "*entity different from the device associated with a called phone number*." *See* element 1.vi.

**i. Claim 9**

> The system recited in claim 1 wherein the security determination comprises determining a validity of the call based at least in part on a cryptographic key on the calling device.

149. The Har/Miller System discloses this claim. First, Har's authentication request and digital signature are "*based at least on part on*" both the caller private key and the authentication server's public key – which are both "*a cryptographic*

*key on the calling device.*" Ex-1004, [0016]. Similarly, Miller's "key" calculated by the encryption function on the device (and thus "on the device") is used for the security determination. *See* 1.iii.(a)/(b), 1.iv, claim 3 *supra*.

**j. Claim 10**

> The system recited in claim 1 wherein the information pertaining to the call further includes a timestamp, and wherein the one or more processors are configured to prevent a replay attack using the timestamp.

150. As detailed in claim 7, Miller discloses a *timestamp*. A POSA would understand a "replay attack" to encompass intercepting and counterfeiting the validation by re-using old data to "replay" a prior validation. Using a "timestamp" to prevent a "replay attack" was well-known in the art. Ex-1020, 16:48-56 ("The timestamp is used to employ a simple logic operation protecting against a replay attack…").

151. Miller addresses the "replay attack" by using the time of the request (timestamp) as a "scoring input" for validity – which is the only "security determination" described in the '989 patent for "replay attacks." Ex-1001, 8:55-60. Moreover, Miller uses different minutia (including time-based minutia) to prevent attacks based upon such "intercepting" of messages and attempted re-use. Ex-1022,

[0041] (Miller "increases the difficulty of spoofing minutia values and intercepting calls intended to counterfeit the original computer."); [0029] (Miller's validation system addresses attempts "[t]o counterfeit a dynamic key crypto-identified computer" which "intercept" messages by detecting "fraudulent response[s]."). Moreover, one method in Miller to prevent such "intercept[ion]" and "fraudulent responses" is to "force the user to enter the user's standard PIN into the computer" which, as detailed for claim 7, uses a time-based assessment. Ex-1022, [0029].

152. Thus, Miller identifies the underlying issues for a replay attack (interception and subsequent fraudulent usage) and describes using the time of the responses for a security determination to detect (and thwart) such replay attacks and therefore renders this claim obvious.

153. Furthermore, a POSA would understand that Miller's "heartbeat" process (described in claim 7) is a well-known method for detecting "replay attacks." "[I]f the heartbeat and chatter 194 process does not perform a valid challenge and response cycle within a timeframe defined by service provider" (indicating a possible replay attack scenario), then the service may be deleted to prevent unauthorized usages. Ex-1022, [0151], [0135].

**k. Claim 11**

> The system recited in claim 1 wherein the security determination is based at least in part on a score indicating a validity of the call, and wherein the score is generated based at least in part on device information.

154. Miller's score is computed at least in part based on "computer minutia" that uniquely identifies the calling device (*generated based at least in part on device information*). See 1.iii.(b) and 1.iv.

**l. Claim 12**

> The system recited in claim 11 wherein the device information used to generate the score comprises at least one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, a user-added hardware identifier, and a device fingerprint.

155. The Har/Miller authentication system renders this claim obvious for the same reasons as 1.iii, 1.iv. The '989 patent references these claim terms in passing. Ex-1001, 9:30-37.

156. Har's "system … supports authentication of mobile devices." Ex-1004, [0044]. As detailed in 1.ii, 1iii and 3, Miller generates its score using a wide variety of computer minutia including (1) "a circuit manufacturer's ID number which may

be readable from a circuit chip element of the computing device" or "memory reads, …clock and other counters, and date" (*embedded hardware identifier*); (2) "which firmware and software codes are installed … and … what particular version or release date of firmware or software are installed …" or "name of the firmware vendor, version number, revision number, revision date, …, and operating system [and] … application name, supplier identification, software release number" (*unique [or] semi-unique software identifier*). Ex-1022, [0031], [0052]. Miller's "[h]ardware minutia values typically cannot change without changing a physical component of the computer" which teaches or renders obvious the "*embedded hardware identifier*." Ex-1022, [0052]. Miller teaches "*user-added hardware*" for the reasons cited below in dependent claim 13.

157. Thus, at a minimum, the Har/Miller authentication server discloses or renders obvious this claim.

158. Miller's minutia details a "*device fingerprint*" in terms very similar to the '989 definition of *device fingerprint*.

| **Miller** | **'989 Patent** |
|---|---|
| A "computer fingerprint typically uses computer minutiae" and Miller's "computer minutia" are sets | "A device 'fingerprint' created from a |

| | |
|---|---|
| of "device manufacturer, model number, serial number, … the name of the firmware vendor, version number, revision number, revision date, …operating system. …. application name, … software release number, … clock and other counters" and "**contact phone numbers**." Ex-1021, [0011], [0052]. | combination of device settings, installed applications, system or application software versions, or **contact list** …." Ex-1001, 9:31-34. |

Miller's "sets" of minutia are used to compute the score as detailed in 1.iii.(b), 1.iv. Thus, Miller discloses the "*device fingerprint*" also.

**m. Claim 13**

> The system recited in claim 12 wherein the user-added hardware identifier is associated with geolocation information.

159. The '939 patent references this claim term obliquely. Ex-1001, 9:29-31 ("user-added hardware identifier like an SD Card or geolocation information"). Miller's "minutia may include such information as geo-location from GPS (global positioning system) capability of the computing device." Ex-1022, [0031]; *see also* Ex-1022, [0040], [0060].

160. PO asserts that this claim is satisfied when "the user-added hardware identifier becomes associated with geolocation information because this information

is stored on the device or about the device." Ex-1007, 120-121. Thus, because Miller stores its geo-location information in both the caller device and on the authentication server in the minutia database in which the "user-added hardware identifier" (from claim 12) is stored, it would be obvious (at least under PO's interpretation) that Miller's "*user-added hardware identifier is associated with geolocation information*." *See* 1.iii, 1.iv, claims 2, 12 (all explaining minutia databases).

**n. Claim 14**

> The system recited in claim 12 wherein the device fingerprint is determined based at least in part on at least one of a set of device settings, a set of installed applications, an indication of a software version, and a contact list.

161. *See* discussion of "*device fingerprint*" in claim 12.

**o. Claim 15**

> The system recited in claim 12 wherein the user-added hardware identifier is associated with a memory card.

162. As detailed in claim 13, PO asserts that a "user-added hardware identifier" "is associated" based upon storage on a device. Miller discloses that its "memory" for its devices and its DKCP includes a wide variety of different media

"E2PROM, FLASH-EPROM, any other memory chip or cartridge." Ex-1022, [0180]. Har's memory includes: "**removable** and non-removable **media** … [and] includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CDROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices." Ex-1004, [0038]. Given the pervasive types of storage described in Miller and Har (particularly "removable"), it would be an obvious implementation that the "*user-added hardware identifiers*" referenced in claim 12 above would be "associated with a memory card" by being stored in a memory card on either the caller device or on Har's authentication server. *See also* Ex-1004, [0042-0047] (detailing the many types of "memory" for Har's mobile devices).

163. Moreover, Miller and Har each disclosure "smartphones" as a caller device. Ex-1004, [0001], [0045]; Ex-1022, [0048]. A POSA would understand that it would be obvious that such smartphones would include *a memory card* such as a "subscriber identity module" card to store information that would render obvious the *user-added hardware identifiers*. Given Miller's teaching of using any computer minutia available on the device, it would be obvious that the information from such a SIM card would be used as minutia available for Miller's DKCP process described above.

**p. Claim 16**

> The system recited in claim 1 wherein the one or more processors are configured to confirm an observed phone number associated with the call.

164. As detailed in 1.iii and 1.iv, the Har/Miller System may use both the caller's phone number and the callee's phone number in the security determination ("*an observed phone number associated with the call*"). Moreover, as detailed in 1.iii, Har describes the ability to use the callee's phone number to contact the callee to solicit a PIN or password to confirm the authenticity of the callee (*confirm an observed phone number associated with the call)*. Ex-1004, [0019], [0035], [0018].

165. Miller's additional authentication includes PIN and/or password verification in checking the "minutia" for verification to confirm participants to the call. Ex-1022, [0054], [0044]. Furthermore, Miller teaches that, in addition to the normal authentication, certain communications may require a PIN verification (consistent with Har's PIN verification). Ex-1022, [0028-0029], [0073], [0122-0129], Fig. 7, [0060] ("user secrets" which includes PIN and password). These each confirm the participants to a communication, such as a call by using the caller or callee communication information (such as a phone number).

166. Thus, at a minimum, each of the Har/Miller verification processes teach, or render obvious, the claimed "*confirm an observed phone number associated with the call*" through their usage of the phone number in the authentication process described above.

167. The "confirm" process in Har and Miller corresponds directly to what the applicant told the Examiner corresponded to claim 16. Claim 16 was prosecution claim 18 which the applicant stated was "support[ed]" by "Paragraph [0054]." Ex-1002, 0145, 0148. "Paragraph [0051]" recites a challenge / response process in which a server sends a communication to a device and receives a response. Ex-1002, 0043, Ex-1001, 10:6-20. The '989 patent process for "confirm[ing]" a phone number corresponds directly to the Har and Miller processes above for contacting a device and receiving confirmation information, such as a PIN.

168. Thus, the Har/Miller System teaches or renders obvious this claim.

**q. Claim 17**

> The system recited in claim 1 wherein the information associated with the call is provided by an agent on the calling device.

169. The "*agent on the calling devic*e" references software, such as an "app" on the calling device. Ex-1001, Figs. 11-15, 5:55-60, 2:48-51. Ex-1002, 0145-0148.

As detailed in Section VII.A.3, the Har/Miller System uses apps or "mobile device authentication modules" on the device to provide the verification information. Ex-1004, Fig. 1; [0021-0024]; Ex-1022, Fig. 1, [0048], [0072].

**r. Claim 18**

> The system recited in claim 1 wherein the information associated with the call is provided in response to one of a detection of an outgoing communication and a prompt to validate communication session information.

170. Har's authentication procedure (and subsequent authentication request) may be performed *in response to detection of* the user's initiation of a voice call. *See* 1.iii, 1.iv. *See also* claim 16 (detailed PIN entry used by Har and Miller to "*prompt to validate communication session information*").

**s. Claim 19**

> The system recited in claim 1 wherein the score is based at least in part on an age of the information associated with the calling device.

171. The Har/Miller System uses *a score based on an age of the information associated with the calling device*. *See* claim 7 (discussion of Miller's timestamp information); claim 10 (discussion of replay attack); Ex-1022, [0055-0056] ("current device image"), claims 21-22.

**t. Claim 20**

> The system recited in claim 1 wherein the score is based at least in part on one or more of feedback associated with a particular phone call, an indication of a stolen device, an indication of a potential spoof attempt, an indication of fraud related to a device, or an indication of a verification that was subsequently determined to be errant.

172. Miller's heuristically-determined "score" is generated based on many factors including "using data from the valid responses DB 130, the SP info and IDs 32 data, the event log 12 and the anticipated minutia DB 98…." Ex-1022, [0105].

> The data modeling, heuristics and permutations 92 process considers historical minutia trends and data mining 94 as well as the current minutia DB 70, the current anticipated minutia DB 98 and the event log 12 which may log actions and exchanges performed by the dynamic key crypto provider 10 for auditing and heuristic analysis at later times

Ex-1022, [0098]. Such "auditing and heuristic analysis" renders obvious that the score is based at least in part on "feedback with a particular phone call" and a "verification that was subsequently determined to be errant."

173. It would be at least obvious for Miller's score be "based at least in part on … an indication of a stolen device, an indication of a potential spoof attempt, an

indication of fraud related to a device" because Miller teaches that the "minutia DB" (used for scoring) keeps track of devices that have been "deleted" or "transferred." Ex-1022, [0163]. This tracking allows the device to "be recognized … if the [device] performs a new registration … maliciously." Ex-1022, [0163].

174. A POSA would recognize that it would be obvious that tracking devices to determine "new registration" from a "deleted" device provides an indication of a stolen device, spoof attempt or fraud related to that device. Thus, by tracking the deleted devices in a database that is used for the scoring, it is obvious that the "*score is based at least in part on one*" of these indications. This is particularly obvious because Miller's system is intended to thwart "spoof" attempts. Ex-1022, [0045], [0041], [0033], [0028], [0011].

**u. Claim 21**

> The system recited in claim 1 wherein the score comprises a reputation score.

175. The '989 patent obliquely references a "reputation score of a caller's device" without any clarification of its meaning. Miller's "compute score 144 process computes a heuristic and probabilistic scoring" using many different factors and "calculates a confidence scoring." Ex-1022, [0105], [0103]. Miller teaches techniques that "uses a complex confidence" to "scor[e] the confidence of a valid

response based on the minutia" that "yields a higher confidence score, increased computer uniqueness, multiple identity factors, and particular minutia isolation" which provides a "confidence rating." Ex-1022, [0030], [0040]; [0022]. The scoring increases "confidence in the computer's uniqueness." Ex-1022, [0034]. See also Ex-1022, [0054] ("confidence rating"); [0106] ("higher confidence scoring"), [0067] ("increase the confidence of a matched result"), [0100] ("scored against a confidence scale").

176. Miller's "confidence scoring" system and evaluation discloses a "reputation score" because it allows varying levels of confidence to be assessed for the device requesting authentication which reflects the device's "reputation" based upon numerous minutia.

**v. Claim 22**

> The system recited in claim 1 wherein the value is generated at least in part by the calling device.

177. The "values" identified in element 1.iii are generated in part by the calling device. For example, Miller's "key" is generated on the device using the cryptography function. Similarly, Har's digital signature and related encryption are also generated on the device. See 1.iii.

**w. Claim 23**

> The system recited in claim 1 wherein the value is provided at least in part by an entity different from the calling device.

178. The Har/Miller System discloses, or renders obvious, this claim because the "*value is provided at least in part by*" a server, such as an authentication server, which is "*an entity different from the calling device*." This "providing by" the authentication server corresponds to the '989 application passages cited to the Examiner during prosecution.

179. Claim 23 was prosecution claim 28 which the applicant stated was supported by Paragraph [0089]. Ex-1002, 0200, 0195, 0054. Paragraph [0089] is Ex-1001, 16:66-17:13. Paragraph [0089] describes a challenge/response process in which a *value is provided… by* the verification service server to the device (such as a "pseudo-random or random number" like a key) and subsequently the "device … in reply, sends a message that makes a reference to at least a portion of the message sent by the verification services provider." Ex-1001, 17:14-17.

180. Har's "authentication request," including its encryption / signature includes values provided by an "*entity different from the calling device*." For example, it would be at least obvious that Har's "keys" used for encryption and

signing would be provided to the device by a different entity – such as a "trusted third party server" that is "part of a public key infrastructure (PKI)." Ex-1004, Abstract, [0016], [0021]. A POSA would understand that both private keys and public keys would be provided by such a trusted server in an asymmetric methodology. Similarly, in Har's embodiment using a "symmetric" key system, it would be obvious that the server provides the "symmetric" key to the device for use in the encryption and signature process.

181. Miller describes a challenge/response sequence similar to that cited to the Examiner for this claim. As detailed in 1.iii and 1.iv, Miller's DKCP provides identification of specific minutia to the device and the device's response includes that minutia (perhaps in its hashed form). Ex-1022, [0058-0067]; Figs. 2A/2B. For example, the hashed response might be "Resp172." Ex-1022, [0066].

182. It would be obvious that the DKCP previously "provided" the possible hashed responses to the devices for the devices to subsequently used. Moreover, the "hashed" values include a random-number component which is provided by a different entity. Ex-1022, [0062] ("The indexes are then combined with a random number using an algorithm defined for each service provider (as described in FIG. 3, specifically the SP info and IDs 32 database)"); [0063] ("combining the indexes with … a random number"); [0071-0074] (describing how the app is *provided by* the

service provider with "unique system encryption keys, unique look up table routines and orderings, different hashing methods for combining minutia values"). It is at least obvious that Miller's hashed and/or encrypted "v*alue is provided* *at least in part by*" the service provider and/or the DKCP in providing the cryptographic materials (including keys) to the device which become a component of the hashed and/or encrypted value returned to the DKCP.

183. Finally, the '989 patent identifies that the value received by the server may be "directly from the device" or "received via another entity (e.g., the entity that was called…"). Ex-1001, 17:18-21. In such indirect communication, the "value is provided … by" the entity in the indirect communication. Miller discloses the exact same ability to indirectly provide the response values from the device to the server. Ex-1022, [0065] ("communicate the response …indirectly via the service provider."). This is a separate teaching corresponding to this claim.

**x. Claim 24**

> The system recited in claim 1 wherein the value comprises at least one of an authentication code, a counter value, a pseudo-random number, a number specific to a particular session, or a number specific to the calling device.

184. The "values" identified in element 1.iii are *authentication codes*, *pseudo-random numbers* and *numbers specific to the calling device*. During prosecution, the applicant cited to paragraphs [0046] and [0089] of the application as support for this claim. Ex-1002, 0195, 0200. Paragraph [0046] teaches "value that may be pseudo-randomly generated, for example, using a key that is stored on the device." Ex-1002, 0041; Ex-1001, 8:48-52.

185. Har's authentication request as encrypted and the associated "digital signature" are each "value(s) … pseudo-randomly generated, for example, using a key that is stored on the device" (the authentication server's public key and the caller private key). Thus, each meets this claim. Similarly, Miller's "key" is generated on the device using the cryptography function and corresponds to a "pseudo-random number." See 1.iii.(a).

186. Miller's minutia (hashed/unhashed and optionally encrypted) is a unique value for authentication (*authentication code*) and *a number specific to the calling device* to provide uniqueness of the device. Similarly, Har's digital signature and encryption is a value that is an *authentication code* and *a number specific to the calling device* (that can be only unlocked using the calling device's public key). *See* 1.iii.

**y. Claim 25**

> The system recited in claim 1 wherein the security determination is performed based at least in part on evaluate of the score against a threshold score.

187. Miller "*evaluate[s] the score against a threshold score*" (or multiple thresholds). Ex-1022, [0111-0120], [0104], Figs. 6A/6B. See 1.iii.(b) and 1.iv.

**z. Claim 26**

> The system recited in claim 1 wherein the score is based at least in part on an age of a timestamp.

188. The Har/Miller System discloses, or renders obvious, this limitation for the same reasons discussed with respect to Claims 7, 10 and 19.

**aa. Claims 27 and 28.**

189. Claims 27 and 28 are the method and computer program product claims corresponding to claim 1 and invalid for the same reasons. Har and Miller each disclose that their functionality is embedded in non-transitory computer readable storage medium and comprises computer instructions. Ex-1004, [0038], [0043], claims 14-20; Ex-1022, [0179-0181], claims 30-34.

190. The following table identifies the analysis in claim 1 that corresponds to each element of claims 27 and 28 according to the Claim Elements Table, *supra*.

| Claim 27, 28 | Claim 1 |
|---|---|
| 27.i, 28.i | 1.i |
| 27.ii, 28.ii | 1.iii |
| 27.iii, 28.iii | 1.iv |
| 27.iv, 28.iv | 1.v |

## CONCLUSION AND DECLARATION

The findings and opinions set forth in this declaration are based on my research and analysis to date. I may continue my examinations in view of additional documents or other factual evidence over the course of this proceeding that may necessitate supplementing and/or refining my opinions. I reserve the right to add to, alter, or delete my opinions and my Declaration upon discovery of additional information. I reserve the right to make such changes as necessary.

In signing this declaration, I understand that the declaration will be filed as evidence in contested case before the Patent Trial and Appeal Board of the United State Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in the case and that cross-examination will take place within the

United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

I declare that all statements made herein on my own knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

[SIGNATURE ON FOLLOWING PAGE]

Declaration of Dr. Patrick McDaniel, Ph.D. 37 C.F.R. § 1.68 in Support of Petition for Inter Partes Review of U.S. Patent No. 11,005,989.

Date: February 9, 2025

Dr. Patrick McDaniel

## APPENDIX A – MATERIALS RELIED UPON

| *Exhibit #* | *Description* |
|---|---|
| **1001** | U.S. Patent No. 11,005,989 ("'989 Patent") |
| **1002** | File History for U.S. Patent No. 11,005,989 |
| **1003** | Expert Declaration of Patrick McDaniel, Ph.D. |
| **1004** | U.S. Patent Publication No. 2012/0144198 ("Har") |
| **1005** | Intentionally Omitted |
| **1006** | Intentionally Omitted |
| **1007** | AT&T Infringement Contentions Exhibit B ('989 Patent), *RightQuestion, LLC v. AT&T Corp., et al.*, No. 2:24-cv-00094-JRG (E.D. Tex.) Served: May 14, 2024. |
| **1008** | Second Amended Docket Control Order in *RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.*, No. 2:24-cv-00091 (E.D. Tex., October 20, 2024) (Lead Case) |
| **1009** | Dave Otway and Owen Rees. 1987. Efficient and timely mutual authentication. SIGOPS Oper. Syst. Rev. 21, 1 (Jan. 1987), 8–10. https://doi.org/10.1145/24592.24594 |
| **1010** | Simpson, E., Schaumont, P. (2006). Offline Hardware/Software Authentication for Reconfigurable Platforms. In: Goubin, L., Matsui, M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_25 ("Simpson") |
| **1011** | Loh Chin Choong Desmond, Cho Chia Yuan, Tan Chung Pheng, and Ri Seng Lee. 2008. Identifying unique devices through wireless fingerprinting. In Proceedings of the first ACM conference on Wireless network security (WiSec '08). Association for Computing Machinery, New York, NY, USA, 46–55. https://doi.org/10.1145/1352533.1352542 |

| ***Exhibit #*** | ***Description*** |
|---|---|
| **1012** | Ke Gao, C. Corbett and R. Beyah, "A passive approach to wireless device fingerprinting," *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, Chicago, IL, 2010, pp. 383-392, doi: 10.1109/DSN.2010.5544294. |
| **1013** | Martins, Rui & Augusto, Alexandre & Correia, Manuel Eduardo. (2013). A Potpourri of Authentication mechanisms - The mobile device way. |
| **1014** | Abu-Hakima, Suhayya, Mansour Toloo and Tony White. "A Multi-Agent Systems Approach for Fraud Detection in Personal Communication Systems." (2002). |
| **1015** | Hossain, A.K.M. Mahtab & Jin, Yunye & Soh, Wee-Seng & Van, Hien. (2013). SSD: A Robust RF Location Fingerprint Addressing Mobile Devices' Heterogeneity. Mobile Computing, IEEE Transactions on. 12. 65-77. 10.1109/TMC.2011.243. |
| **1016** | AT&T Infringement Contentions Cover Pleading, *RightQuestion, LLC v. AT&T Corp., et al.*, No. 2:24-cv-00094-JRG (E.D. Tex.) Served: May 14, 2024. |
| **1017** | Boris Danev (2011) Physical-Layer Identification of Wireless Devices [Doctoral dissertation, ETH Zurich]. ETH Zurich Library Collection. https://www.research-collection.ethz.ch/handle/20.500.11850/72822 |
| **1018** | Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. ACM Comput. Surv. 45, 1, Article 6 (November 2012). https://doi.org/10.1145/2379776.2379782 |
| **1019** | Intentionally Omitted |
| **1020** | U.S. Pat. No. 9,129,130 (Filed: August 30, 2013; Priority: August 31, 2012) |
| **1021** | Intentionally Omitted |
| **1022** | U.S. Patent Publication No. 2012/0201381 ("Miller") |
| **1023** | Joint Claim Construction Statement, RightQuestion, LLC v. AT&T Corp., et al., No. 2:24-cv-00094-JRG (E.D. Tex.) |

| ***Exhibit #*** | ***Description*** |
|---|---|
| **1024** | U.S. Patent Publication No. 2007/0219801 (filed March 14, 2006, published September 20, 2007). |

# APPENDIX B – CURRICULUM VITAE

# Patrick Drew McDaniel

Tsun-Ming Shih Professor of Computer Sciences
School of Computer, Data and Information Sciences ⋄ University of Wisconin-Madison
*Office* : Room 7387, 1210 W. Dayton St. ⋄ Madison, WI 53706 ⋄ (608) 263-1008
*email*: mcdaniel@cs.wisc.edu ⋄ *Homepage*: `https://patrickmcdaniel.org/`


## ACADEMIC AND RESEARCH APPOINTMENTS

**Tsun-Ming Shih Professor of Computer Sciences**, 2022-Present
University of Wisconsin-Madison, Madison, WI

**William L. Weiss Professor of Information and Communications Technology** 2017-2022
Computer Science and Engineering, Pennsylvania State University, University Park, PA

**Distinguished Professor** 2016-2017
Computer Science and Engineering, Pennsylvania State University, University Park, PA

**Professor** 2011-2015
Computer Science and Engineering, Pennsylvania State University, University Park, PA

**Associate Professor** 2007-2011
Computer Science and Engineering, Pennsylvania State University, University Park, PA

**Hartz Family Career Development Assistant Professor** 2004-2007
Computer Science and Engineering, Pennsylvania State University, University Park, PA

**Adjunct Professor** 2003-2009
Stern School of Business, New York University, New York, NY

**Senior Research Staff Member** 2001-2004
AT&T Labs - Research, Florham Park, NJ

## RESEARCH LEADERSHIP APPOINTMENTS

**Director, National Science Foundation, Center for Trustworthy Machine Learning** 2018-present
Participants: Penn State, Stanford, UC Berkeley, UC San Diego, Univ. of Wisconsin, Univ. of Virginia

**Director, Institute for Networking and Security Research** 2016-2022
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

**Program Manager, Cyber-Security Collaborative Research Alliance (CRA)** 2013-2018
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

**Co-Director, Systems and Internet Infrastructure Laboratory** 2004-2022
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

## EDUCATION

Ph.D., Computer Science and Engineering, **University of Michigan**, Ann Arbor, MI 2001
M.S., Computer Science, **Ball State University**, Muncie, IN 1991
B.S., Computer Science **Ohio University**, Athens, OH 1989

## AFFILIATIONS

Association for Computing Machinery (ACM), *Fellow*

The Institute of Electrical and Electronics Engineers (IEEE), *Fellow*

American Association for the Advancement of Science (AAAS), *Fellow*

USENIX Advanced Computing Systems Association (USENIX)

## STUDENTS

### Past PhD Students

- *Z. Berkay Celik*, Spring 2019, now **Assistant Professor**, Purdue University




EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0102

- *Nicolas Papernot*, Spring 2018, now **Assistant Professor**, University of Toronto
- *Wenhui Hu*, Fall 2016, now **Senior Member of Technical Staff**, Oracle
- *Devin Pohly*, Spring 2016, now **Assistant Professor**, Wheaton College
- *Damien Octeau*, Summer 2014, now **Software Engineer in Security**, Google
- *Steve McLaughlin*, Spring 2014, now **Senior Software Engineer**, Samsung Research America
- *Thomas Moyer*, Summer 2011, now **Assistant Professor**, University of North Carolina-Charlotte
- *William Enck*, Spring 2011, now **Professor**, North Carolina State University
- *Kevin Butler*, Summer 2010, now **Professor**, University of Florida
- *Machigar Ongtang*, Summer 2010, now **Assistant Professor**, Dhurakij Pundit University
- *Patrick Traynor*, Spring 2008, now **John and Mary Lou Dasberg Preeminent Chair, Professor**, University of Florida, co-advisor
- *Fr. Boniface Hicks*, Fall 2007, now **Assistant Professor**, St. Vincent College

**Current PhD Students**

- *Jean-Charles Noirot Ferrand*, University of Wisconsin, Spring 2028
- *Kyle Domico*, University of Wisconsin, Spring 2028
- *Kunyang Li*, University of Wisconsin, Spring 2027
- *Rachel King*, University of Wisconsin, Spring 2027
- *Yohan Beugin*, University of Wisconsin, Spring 2026
- *Blaine Hoak*, University of Wisconsin, Spring 2026
- *Quinn Burke*, University of Wisconsin, Spring 2026
- *Eric Pauley*, University of Wisconsin, Spring 2025
- *Ryan Sheatsley*, University of Wisconsin, Spring 2024

**Past Masters Students**

- *Blaine Hoak*, Pennsylvania State University, Summer 2022
- *Rachel King*, Pennsylvania State University, Summer 2022
- *Alban Heon*, Pennsylvania State University, Summer 2022
- *Yohan Beugin*, Pennsylvania State University, Spring 2021
- *Ahmed Abdou*, Pennsylvania State University, Spring 2021
- *Adrien Cosson*, Pennsylvania State University, Summer 2020
- *Bolor Zolbayar*, Pennsylvania State University, Summer 2020
- *Alejandro Andrade*, Pennsylvania State University, Summer 2020
- *Quinn Burke*, Pennsylvania State University, Spring 2020
- *Eric Pauley*, Pennsylvania State University, Spring 2020
- *Sushrut Shringarputal*, Pennsylvania State University, Fall 2019
- *Raquel Alvarez*, Pennsylvania State University, Spring 2019
- *Valentin Vie*, Pennsylvania State University, Spring 2019
- *Ryan Sheatsley*, Pennsylvania State University, Fall 2018
- *Eric Kilmer*, Pennsylvania State University, Spring 2016
- *Nathan Lagerman*, Pennsylvania State University, Spring 2016
- *Matthew Dering*, Pennsylvania State University, Spring 2014
- *Phil Koshy*, M.S. Pennsylvania State University, Fall 2013
- *Diana Koshy*, M.S. Pennsylvania State University, Fall 2013
- *Steve McLaughlin*, M.S. Pennsylvania State University, Spring 2011
- *Sergei Miadzvezhanka*, M.S. Pennsylvania State University, Spring 2011
- *Adam Delozier*, M.S. Pennsylvania State University, Spring 2011
- *Juliet Uhlott*, M.Eng. Pennsylvania State University, Fall 2010



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0103

- *Damien Octeau*, M.S. Pennsylvania State University, Spring 2010
- *Thomas Moyer*, M.S. Pennsylvania State University, Spring 2009
- *Luke St. Clair*, M.S. Pennsylvania State University, Summer 2008
- *Lisa Johansen*, M.S. Pennsylvania State University, Spring 2008
- *Sunam Ryu*, M.S. Pennsylvania State University, Spring 2007
- *Dhananjay Bapat*, M.S. Pennsylvania State University (Electrical Engineering), Fall 2006
- *Jennifer Plasterr*, M.Eng. Pennsylvania State University, Summer 2006
- *Adam Kerr*, M.Eng. Pennsylvania State University, Fall 2006
- *William Enck*, M.S. Pennsylvania State University, Spring 2006
- *Wesam Lootah*, M.S. Pennsylvania State University, Spring 2006
- *Jon Hansford*, M.Eng. Pennsylvania State University, Fall 2005
- *John van Bremer*, M.Eng. Pennsylvania State University, Spring 2005

**Past Post-Docs**

- *Vaibhav Rastogi*, graduated Northwestern University
- *Robert Walls*, graduated University of Massachusetts, Amherst

## TEACHING

**University of Wisconsin-Madison, College of Letters and Science**

- **Intro to Information Security** - Fall 2023

**Pennsylvania State University, College of Engineering**

- **CMPSC311 - Introduction to Systems Programming** - Fall 2013, Fall 2014, Fall 2015, Fall 2016, Summer 2019, Spring 2020, Fall 2020, Fall 2021
- **CMPSC443 - Introduction to Computer and Network Security** - Spring 2006, Spring 2009, Fall 2017, Fall 2018
- **CSE543 - Computer and Network Security** - Fall 2004, Fall 2005, Fall 2008, Fall 2009, Fall 2011, Fall 2014
- **CSE544 - Advanced System Security** - Spring 2005, Spring 2007
- **CSE545 - Advanced Network Security** - Spring 2006, Spring 2008, Spring 2011
- **CSE597g - Principles, Analysis, and Applications of Computer Security** - Fall 2015
- **Security and Privacy of Machine Learning** - Fall 2016
- **Advanced Topics in the Security and Privacy of Machine Learning** - Spring 2017
- **CSE598 - Cell Phone Operating Systems** - Spring 2009
- **CSE598i - Web 2.0 Security** - Spring 2010
- **CSE598d - Topics in Applied Systems Security** - Fall 2010
- **CSE598e - Critical Infrastructure Security** - Fall 2011
- **CSE 597 – Emerging Trends in Computer Security** - Fall 2021
- **CMPSC297 – Introduction to C Programming in UNIX** - Fall 2021

**New York University, Stern School of Business**

- **B20.3157 Computer and Network Security** - Spring 2003, Summer 2004, Summer 2005
- **B20.3156 - Online Privacy** - Spring 2003, Summer 2004



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0104

## HONORS, AWARDS, AND KEYNOTE ADDRESSES

**SIGSAC Outstanding Innovation Award**, *for innovative research in mobile device security, trustworthiness of machine learning, and systems security, November 2021*

**Penn State Engineering Society Premier Research Award**, *Given to one faculty member per year, the Penn State Engineering Alumni Society Premier Research Award recognizes and rewards an individual whose contributions to scientific knowledge through research are exemplary and internationally acclaimed, April 2021*

**AAAS Fellow**, *for distinguished contributions to the field of computational security and privacy, particularly for advancing algorithms for the formal analysis of mobile devices and applications, November 2020*

**SIGOPS Hall of Fame Award**, *recognizing the paper "TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones" (Will Enck first author), "which sparked an important research agenda on smartphone privacy that continues to this day", November 2020*

**J. D. Williams student paper award, Nuclear Security and Physical Protection division**, *recognizing the best student papers by area in Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July 2019*

**Penn State Engineering Society Outstanding Advising Award**, *highly selective award by the Penn State Engineering Society given to faculty in the College of Engineering who have made significant contributions as advisor, October 2018*

**Best Paper, 2017 EAI SECURECOMM 2018**, *with Sayed M. Saghaian, Tom La Porta, Trent Jaeger and Z. Berkay Celik, August 2018*

**Best Student Paper, 2017 ACM Symposium on SDN Research (SOSR)**, *with Stefan Achleitner, Thomas La Porta and Trent Jaeger, April 2017*

**IEEE Technical Committee on Security and Privacy Outstanding Community Service Award**, *in recognition for leadership of the Technical Committee on Security and Privacy, May 2016*

**ACM Fellow**, *for contributions to computer and mobile systems security, December 2015*

**Science of Security Index of Significant Research in Cyber Security** , *acknowledging paper 'Toward a Science of Secure Environments', Science of Security Virtual Organization (SOS-VO), August 2015*

**IEEE Fellow**, *for contributions to the security of mobile communications, November 2014*

**Best Artifact Award, 20th International Symposium on the Foundations of Software Engineering (FSE)**, *with advisee Damien Octeau and collaborator Somesh Jha, November 2012*

**Best Paper, 25th Annual Computer Security Applications Conference**, *with advisees Machigar Ongtang, Stephen McLaughlin, and William Enck, December 2009*

**Faculty Marshal, College of Engineering**, *selected by student marshals for contributions to undergraduate education, leads procession into graduation ceremony, May 2009*

**Penn State Engineering Society Outstanding Research Award**, *highly selective award by the Penn State Engineering Society given to faculty in the College of Engineering who have made significant contributions to knowledge in their field, March 2009*

**Google Security and Product Safety Acknowledgement**, *in recognition of efforts in improving the security of Google Android cellular phone operating system, 2008*

**Commendation for Exceptional Leadership and Achievement** , *in recognition of efforts as PI of the EVEREST study, from Ohio Secretary of State Jennifer Brunner, August 2008*

**IEEE Technical Committee on Security and Privacy Outstanding Community Service Award**, *in recognition for technical program management of the IEEE Security and Privacy symposia, August 2008*

**National Science Foundation CAREER Award**, *Faculty early career development grant, August 2007*

**Penn State Computer Science and Engineering Outstanding Teaching Award**, *Given to best teacher in the department as selected by students, March 2007*

**ACM Certificate of Meritorious Service**, *Certificate acknowledging exemplary service as associate editor of ACM Transactions on Internet Technologies, April 2007*



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0105

**Best Student Paper, 22nd Annual Computer Security Applications Conference**, *as advisor, with Boniface Hicks and Kiyan Ahmadizadeh, December 2006*

**Best Paper, Innovations and Commercial Applications of Distributed Sensor Networks Symposia**, *Awarded for best paper in conference, October 2005.*

**Hartz Family Career Development Professor**, *Endowed Professorship, Pennsylvania State University, Fall 2004-2007*

**Bang for the Buck Award, DARPA Dynamic Coalitions Program**, *Award for most feature-rich/useful software system, April 2002*

**National Aeronautics and Space Administration, Kennedy Space Center Fellowship**, *Research Fellowship, September 1997 - August 2000*

**Electrical Engineering and Computer Science Summer Fellowship Award**, *University of Michigan, June 1997*

**Dean's Citation for Perfect Academic Record**, *Ball State University, June 1991*

**Keynote Addresses**

1. Securitys Role in Achieving Sustainability, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.
2. Security, Game Theory, and Their Role in Achieving Sustainability, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.
3. Prognosticating the Future of IoT Security, 2022 IEEE SafeThings Workshop, San Francisco, CA, May 2022.
4. The Challenges of Machine Learning in Adversarial Settings. Triangle Area Privacy and Security Day, Durham, NC, October, 2019.
5. The Challenges of Machine Learning in Adversarial Settings. 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.
6. Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings. 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.
7. Tracing the Arc of Smartphone Application Security. 2017 ACM on International Workshop on Security And Privacy Analytics. Scottsdale, AZ, March, 2017.
8. Tracing the Arc of Smartphone Application Security. 12th International Conference on Information Systems Security, Jaipur, India, December, 2016.
9. The 25th International Conference on Computer Communication and Networks (ICCCN 2016), August, 2016, Waikoloa, Hawaii.
10. Learning from Ourselves: Where are we and where can we go in mobile systems security?. Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.
11. Eight Years of Mobile Smartphone Security. Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.
12. The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security (CNS), September 2015, Florence, Italy.
13. The Importance of Measurement and Decision Making to a Science of Security. 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.
14. The Importance of Measurement and Decision Making to a Science of Security, 2015 Symposium And Bootcamp on the Science of Security (Hotsos), April 2015, University of Illinois at Urbana-Champaign



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0106

15. Security and Science of Agility, ACM Workshop on Moving Target Defense (MTD 2014), November 2014, Scottsdale, AZ

16. A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape, IEEE New Technology Industry Seminar (NTIS '13), Everett WA, August, 2013

17. Permission-based Application Governance; A Step Forward or Backward?, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July 2012.

18. Scalable Integrity-Guaranteed AJAX, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April 2012.

19. Security Challenges and Solutions in Mobile Smartphone Applications, IEEE Computer Security Foundations (CSF 2011), Abbaye des Vaux de Cernay, France, June 2012.

20. Password Exhaustion: Predicting the End of Password Usefulness. 2nd International Conference on Information Systems Security, Kolkata India, December, 2006.

21. Physical and Digital Convergence: Where the Internet is the Enemy. Eighth International Conference on Information and Communications Security (ICICS '06), Raleigh, NC, December, 2006.

**Distinguished Lectures**

1. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Michigan State University, Lansing, MI, November, 2023.

2. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, Temple University, Philadelphia, PA, February, 2022.

3. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.

4. Shutterstock Distinguished Lecture: The Challenges of Machine Learning in Adversarial Settings. Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.

5. Distinguished Blockchain Lecture: The Challenges of Machine Learning in Adversarial Settings. Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.

6. Distinguished Speaker Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.

7. Samuel D. Conte Distinguished Lecture Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, Purdue University, West Lafeyette, Indiana, November, 2018.

8. The Challenges of Machine Learning in Adversarial Settings. Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

9. Tracing the Arc of Smartphone Application Security. Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

10. Tracing the Arc of Smartphone Application Security. Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Colins, CO, October, 2017.

11. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

12. Tracing the Arc of Smartphone Application Security, University of Texas-Dallas Department of Computer Science, Dallas, TX, May 2017.

13. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, May 2017.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0107

14. Tracing the Arc of Smartphone Application Security. University of California-Irvine, Computer Science Department, Irvine CA, March, 2017.

15. Tracing the Arc of Smartphone Application Security. The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

16. Tracing the Arc of Smartphone Application Security. Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

17. Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrucken Germany, July, 2015.

18. Six Years of Mobile Smartphone Security. Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

19. Security Challenges and Solutions in Mobile Smartphone Applications. Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

20. Security Challenges and Solutions in Mobile Smartphone Applications. Department of Software Information Systems College of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

## RESEARCH SUPPORT

**co-PI**, *MURI: Cohesive and Robust Human-Bot Cybersecurity Teams*, Army Research Office, *$6,000,0000* (PSU award $739,527), 07/01/2021-06/30/2026, Collaborators: Many.

**co-PI**, *SaTC: CORE: Small: Adversarial Network Reconnaissance in Software Defined Networking*, NSF (CNS), *$500,000* (PSU award $500,000), 1/1/2020-12/31/2022, Collaborators: He (Penn State).

**PI**, *CNS Core: Medium: Automated IoT Safety and Security Analysis and Synthesis*, NSF (CNS), *$272,033* (PSU award $272,033), 6/25/2019-6/24/2022, Collaborators: Tan (Penn State).

**PI**, *Mapping Black-Box Attack Metrics and Parameter Spaces in Machine Learning*, US Army Aviation and Missile Research, Development and Engineering Center, *$436,677* (PSU award $436,677), 6/25/2019-6/24/2022, Collaborators: (single PI).

**PI**, *SaTC CORE: Frontier: Collaborative: End-to-End Trustworthiness of Machine-Learning Systems*, NSF (CNS), *$9,649,366* (PSU award $2,044,550), 8/15/2018-3/31/2023, Collaborators: Boneh (Stanford), Chaudhuri (UCSD), Evans (Virginia), Jha (Wisconsin), Liang (Stanford), Song (Berkeley).

**PI**, *2017 SaTC PI Meeting*, NSF (CNS), *$99,999* (PSU award $50,230), 8/15/2016-3/31/2017, Collaborators: Antonakakis (GaTech), Mason (UIUC).

**PI**, *TWC: Medium: Collaborative: Scaling and Prioritizing Market-Sized Application Analysis*, NSF (CNS), *$1,147,213* (PSU award $547,213), 7/01/2016-6/30/2020, Collaborators: Jha (Wisconsin).

**PI**, *Student Travel Support for Symposium on Security and Privacy 2014*, Army Research Office, *$10,000* (PSU award $10,000), 5/1/14-5/1/15.

**PI**, *Models for Enabling Continuous Reconfigurability of Secure Missions (MACRO) Cyber-Security Collaborative Research Alliance (CRA)*, Army Research Laboratory, *$24.1 million ($48.2 million with renewal at 12/17)*, 9/20/2013-9/19/2023 (renewed at 5 years), Collaborators: PSU, Carnegie Mellon, Indiana, UC Davis, UC Riverside, ARL, CERDEC.

**PI**, *Google Faculty Research Award, Plotting a Map of Android Inter-App Communication*, Google, *$50,000*, 3/1/2012-2/28/2013, Collaborators: PSU (McDaniel), TU Darmstadt (Bodden), University of Luxembourg (Traon), .

**PI**, *Battelle BGP Security Study (Phase 2)*, Battelle, *$102,815*, 10/1/2012-9/30/2013, Collaborators: PSU (McDaniel), Oregon (Butler).

**PI**, *TWC: Medium: Collaborative: Extending Smart-Phone Application Analysis*, NSF (CNS), *$1,386,518 (plus 16k REU supplement)* (PSU award $534,748), 8/1/2012-7/31/2016, Collaborators: PSU (McDaniel), Wisconsin (Jha).



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0108

**PI**, *Battelle BGP Security Study (Phase 1)*, Battelle, *$94,400*, 2/15/2012-9/30/2012, Collaborators: PSU (McDaniel).

**co-PI**, *TC: Medium: Collaborative Research: Building Trustworthy Applications for Mobile Devices*, NSF (CNS), *$1,386,518* (PSU award $350,000), 8/1/2011-7/31/2014, Collaborators: PSU (McDaniel), Wisconsin (Banerjee, Jha, Swift).

**PI**, *Closing the Loop on Security Testing and Security Requirements*, Security and Software Engineering Research Center, *$31,000*, 8/1/2011-7/31/2012.

**co-PI**, *Managing Security and Vulnerability Risks in the Smart Grid*, Institute for CyberScience and The Penn State Institutes of Energy and the Environment, *$31,000*, 08/1/09-12/16/09, Collaborators: PSU (Blumsack, McDaniel).

**PI**, *Smart Grid Cyber Security Research*, Lockheed Martin, *$250,000*, 1/1/10-12/16/10.

**PI**, *NSF HECURA: Collaborative Research: Secure Provenance in High-End Computing Systems*, NSF (CCF), *$1,000,000* (PSU award $307,073), 08/1/09-8/31/13, Collaborators: PSU (McDaniel), UIUC (Winslett), Stonybrook (Sion, Zadok).

**PI**, *TC: Medium: Collaborative Research: Security Services in Open Telecommunications Networks*, NSF (CNS), *$1,386,518* (PSU award $594,941), 08/01/09-08/01/12, Collaborators: PSU (McDaniel, La Porta), UPenn (Blaze), Columbia (Schulzrinne).

**PI**, *Characterizing and Mitigating Wireless Systems Vulnerabilities*, Defense University Research Instrumentation Program (DURIP), Army Research Office (ARO), *$150,000*, 05/22/09-02/28/11, Collaborators: PSU (La Porta, McDaniel).

**co-PI**, *Integrity Management for ICT Development*, Bell Labs Network Reliability and Security Office, Alcatel-Lucent , *$100,000*, 11/30/08-11/30/09, Collaborators: PSU (La Porta, McDaniel).

**PI**, *Utility Grid Automation and Risk Management*, Lockheed Martin, *$400,000*, 11/30/08-12/16/09.

**PI**, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing*, The State of Ohio, *$716,336* (PSU award $332,066), 10/01/07-01/07/08, Collaborators: PSU (McDaniel), UPenn (Blaze), UCSB (Kemmerer, Vigna), Berkeley (Hall, Quilter).

**Co-PI**, *Protecting Services for Emerging Wireless Telecommunications Infrastructure*, NSF (CNS), *$658,032*, 09/01/07-08/31/11, Collaborators: PSU (La Porta, Jaeger, McDaniel).

**Co-PI**, *Security for Internet/IMS Convergence*, Cisco, *$100,000*, 9/1/07-8/31/08, Collaborators: PSU (La Porta, McDaniel).

**Co-PI**, *System-Wide Information Flow Enforcement*, BAA 06-11-IFKA, "National Intelligence Community Enterprise Cyber Assurance Program", *$496,000*, 2/1/07-8/1/08, Collaborators: PSU (Jaeger, McDaniel).

**PI**, *CAREER: Realizing Practical High Assurance through Security-Typed Information Flow Systems*, NSF (CNS), *$400,000*, 1/2/07-1/1/12.

**Co-PI**, *CT-IS: Shamon: Systems Approaches for Constructing Distributed Trust*, NSF (CNS), *$400,000*, 9/1/06-8/31/10, Collaborators: PSU (Jaeger, McDaniel).

**Co-PI**, *Center of Excellence*, Ben Franklin Technology Partners, *$75,000*, 01/01/07-07/01/07, Collaborators: PSU (Cao, Jaeger, La Porta, McDaniel, Smith).

**Co-PI**, *Exploiting Asymmetry in Performance and Security Requirements for I/O in High-end Computing*, NSF (CFF), *$699,690*, 9/1/06-8/31/10, Collaborators: PSU (McDaniel, Sivasubramaniam).

**PI**, *Automated Configuration with the PRESTO Network Management Platform*, AT&T, *$100,000*, 6/1/06-5/31/07.

**PI**, *Testbed for Network-Scale Countermeasure Evaluation*, Cisco, *$45,938*, 9/1/05-8/31/06.

**PI**, *Collaborative Research: CT-T: Flexible, Decentralized Information-flow Control for Dynamic Environments*, NSF (CFF), *$1,057,427* (PSU award $234,585), 8/1/05-7/31/08, Collaborators: PSU (McDaniel), UPenn (Zdancewic), Maryland (Hicks), GMU (Winsborough).

**PI**, *Extending Developer Tools for Security-typed Languages*, Software Engineering Research Center, Sponsor: Motorola, *$23,200*, 7/1/05-6/30/06.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0109

**PI**, *Student Travel Support for ACM SIGCOMM 2005 Conference*, NSF, *$19,620*, 4/1/05-3/31/06.

**Co-PI**, *NSF CyberTrust: Collaborative Research: Testing and Benchmarking Methodologies for Future Network Security Mechanisms (EMIST)*, NSF/DHS, *$5,344,459* (PSU award $2,533,447), 8/1/04-8/31/06, Collaborators: PSU (Kesidis, Miller, Liu), Purdue (Fahmy, Rosenberg, Spafford, Shroff, Brodley), UCDavis (Wu, Levitt, Bishop, Rowe), ICSI/Berkeley (Paxson, Floyd, Weaver).



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0110

# PROFESSIONAL ACTIVITIES

## Editorial Positions, Panels, and Boards

**IEEE Technical Committee on Security and Privacy**

- *Chair*–January 2014-January 2016
- *Vice Chair*–January 2012-December 2014

**ACM Transactions on Internet Technology (TOIT)**

- *Editor in Chief*–September 2007-December 2012
- *Associate Editor*–April 2004-August 2007

**IEEE Security and Privacy Magazine**

- *Area Editor, Secure Systems*–January 2009-2015

**IEEE Transactions on Computers (TC)**

- *Associate Editor*–August 2008-2014

**ACM Transactions on Information and System Security (TISSEC)**

- *Associate Editor*–May 2007-May 2012

**IEEE Transactions on Software Engineering (TSE)**

- *Associate Editor*–January 2007-April 2012
- *Guest Editor, Special Issue on Topics in Security*–Fall 2006-April 2012

**IEEE Transactions on Parallel and Distributed Systems (TPDS)**

- *Guest Editor, Special Issue on Trust, Security and Privacy in Parallel and Distributed Systems*–Fall 2012

**Elsevier Journal of Computer Networks**

- *Guest Editor, Special Issue on Web Security*–Fall 2003-Spring 2005

**Encyclopedia of Cryptography and Security**

- *Editorial Board Member*–Fall 2002-Spring 2005

**Journal of Defense Modeling and Simulation**

- *Guest Editor, Special Issue on Cyber Risk and Vulnerability Estimation*–Winter 2018-

## Other Professional Activities

**IEEE Workshop on the Internet of Safe Things (SafeThings)**

- *Steering Committee*–2022-present

**Helmholtz Center for Information Security (CISPA), Scientific Advisory Board**

- *Member*–2019-present

**Ohio University College of Engineering, Board of Vistors**

- *Member*–2018-present

**Penn State CISO Advisory Board**

- *Member*–2016-2022

**Member, Technical Guideline Development Committee, U.S. Election Assistance Commission**

- *Member*–2010-2011

**Natural Sciences and Engineering Research Council of Canada, Internetworked Systems Security Network**

- *Scientific Advisory Board*–2008-2013

**Technology for Cyber Physical System Security Forum, Cyber Security Research and Development, (Senators Joseph I. Lieberman and Susan Collins, Chairs)**

- *Speaker and Participant*–September 2008

**ACM Student Organization Advisor**

- *Penn State Computer Science and Engineering Department*–2006-2012

**The Technology Collaborative**

- *Penn State Representative (Pennsylvania economic development consortium)*–2007-2008



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0111

**President's National Security Telecommunications Advisory Panel**

- *Member, Next Generation Networks Task Force*–2005-2006

**Abusable Technologies Awareness Center (ATAC)**

- *Panelist*–October 2003-2010

**AT&T IP Services Security Council**

- *Member*–June 2003-August 2004

**AT&T Internet Intellectual Property Review Team**

- *Member*–September 2001-May 2002

**ACM SIGCOMM Student Travel Grant Committee**

- *Member*–August 2005

**National Science Foundation, Grant Review Panel**

- *Member*–2003-2004, 2006-2007, 2009-2021

**Department of Energy SciDAC Review Panel**

- *Member*–2001

## Conference and Workshop Participation

**IEEE Symposium on Security and Privacy**

- *Technical Program Co-Chair*–2007, 2008
- *Program Committee*–2011, 2012, 2013, 2022, 2023, 2024

**USENIX Security Symposium**

- *Program Chair*–2005
- *Invited Talks Chair*–2006, 2009
- *Program Committee*–2001, 2003, 2004, 2007, 2014, 2018, 2019, 2020, 2021, 2022, 2023, 2024

**ACM Conference on Computer and Communications Security (CCS)**

- *Program Committee*–2006, 2008, 2009, 2010, 2012, 2018, 2019, 2020, 2021, 2022, 2023
- *Industry and Government Track Chair*–2004, 2007
- *Program Committee-Industry and Government Track*–2003, 2005, 2006
- *Test of Time Committee*–2019, 2020

**IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)**

- *Founding Program Co-Chair*–2023

**IEEE European Symposium on Security and Privacy**

- *Steering Committee*–2015-present
- *Program Committee*–2016, 2017

**International Conference on Privacy, Security and Trust (PST)**

- *Steering Committee*–2019-

**ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)**

- *Program Committee*–2017

**Network and Distributed System Security Symposium (NDSS)**

- *Program Committee*–2009, 2012, 2013, 2017

**Annual Computer Security Applications Conference (ACSAC)**

- *Program Committee*–2004, 2005, 2006, 2007, 2010, 2011, 2019
- *Test of Time Committee*–2019

**Financial Cryptography**

- *General Chair*–2006
- *Program Committee*–2007, 2008, 2012

**Computer Security Foundations Symposium (CSF)**

- *Program Committee*–2011, 2021

**European Symposium on Research in Computer Security (ESORICS)**



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0112

- *Program Committee*–2004, 2005, 2021

**ACM Symposium of SDx Research 2021 (SOSR)**
- *Program Committee*–2021

**International Symposium on Engineering Secure Software and Systems (ICISSP)**
- *Program Committee*–2015

**IEEE Conference on Communications and Network Security (CNS)**
- *Program Committee*–2015, 2017

**ACM Annual International Conference on Mobile Computing and Networking (MobiCom)**
- *Program Committee*–2010, 2011, 2012
- *Program Committee, Distinguished Member*–2021

**ACM Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)**
- *Program Committee*–2012

**ACM Symposium on Access Control Models and Technologies (SACMAT)**
- *Program Committee*–2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2011

**ACM Conference on ASIA Computer and Communications Security (ASIA CCS)**
- *Program Committee*–2008

**ACM Conference on Electronic Commerce (ACM EC)**
- *Program Committee*–2005

**EAI International Conf. on Security and Privacy in Communication Networks (SecureComm)**
- *Program Committee*–2020

**International Conference on Applied Cryptography and Network Security (ACNS)**
- *Program Committee*–2006

**ACM Annual Digital Forensics Conference**
- *Program Committee*–2012

**IEEE Workshop on the Internet of Safe Things**
- *Program Committee*–2019, 2022

**ACM Workshop on Moving Target Defense (MTD)**
- *Program Committee*–2015, 2016

**IEEE ICNP Workshop on Secure Network Protocols (NPSec)**
- *Program Committee*–2005, 2006

**Conference on Decision and Game Theory for Security (GameSec)**
- *Program Committee*–2012, 2018

**ACM Symposium on Applied Computing (SAC)**
- *Program Committee, Information Security Research and Applications* –2010

**USENIX Annual Technical Conference**
- *Program Committee*–2002, 2003

**World Wide Web Conference (WWW)**
- *Security and Privacy Track Vice-Chair*–2005
- *Security and Privacy Track Deputy Vice-Chair*–2004
- *Program Committee*–2003, 2007, 2010, 2011

**Intl. Conference on Emerging Trends in Information and Communication Security (ETRICS)**
- *Program Committee*–2006

**International Conference On Distributed Computing Systems (ICDCS)**
- *Program Committee*–2011

**IEEE INFOCOM**
- *Program Committee*–2007

**IEEE GLOBECOM**
- *Program Committee*–2010

**Military Communications Conference (MILCOM)**



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0113

- *Program Committee*–2015, 2016, 2017, 2018, 2019, 2021, 2022

**The Five Nines Workshop on Designing and Managing High Availability Internet Services (INM)**
- *Program Committee*–2007

**International Conference on Information Systems Security (ICISS)**
- *Steering Committee*–2007
- *Program Co-Chair*–2007
- *Program Committee*–2005, 2006, 2009, 2011

**International Conference on Parallel Processing**
- *Program Committee-Network Security*–2003

**USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)**
- *Program Committee*–2010

**ACM Workshop on Networking, Systems, Applications on Mobile Handhelds (MobiHand)**
- *Program Committee*–2009

**ACM Workshop on Cloud Computing Security**
- *Program Committee*–2009, 2010

**ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)**
- *Program Committee*–2011, 2012, 2013

**International Workshop on Security in Software Engineering**
- *Founding General Co-Chair*–2007

**USENIX Workshop On Offensive Technology (WOOT)**
- *Program Committee*–2007

**ACM Storage Security and Survivability Workshop**
- *Program Committee*–2006

**ACM SIGCOMM Workshop on Internet Network Management**
- *Program Committee*–2006, 2007

**Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)**
- *Program Committee*–2006, 2007, 2008

**Workshop on Workshop on Telecommunications Infrastructure Protection and Security (TIPS)**
- *General Chair*–2009

**USENIX Workshop on Hot Topics in Security (HotSec)**
- *Program Chair*–2011
- *Program Committee*–2007, 2008, 2009, 2010, 2012

**ACM Workshop TPC on Security and Privacy in Smartphones and Mobile Devices**
- *Program Committee*–2011

**International Workshop on Security (IWSEC)**
- *Program Committee*–2006

**International Workshop on Systems and Network Security (SNS)**
- *Program Committee*–2005, 2006

## COLLABORATORS (Last 48 Months)

Bolor-Erdene Zolbayar , Ahmed Abdou, Stefan Achleitner, Hidayet Aksu, Leonardo Babun, Paul Barford, Novella Bartolini, Yohan Beugin, Hoak, Blaine, Christopher Burchard, Quinn Burke, Z. Berkay Celik, Kamalika Chaudhuri, Adrien Cosson, Kyle Denney, Genannt Dohmann, Kyle Domico, Kyle D Domico, Matthew Durbin, Pauley, Eric, David Evans, Jean-Charles Noirot Ferrand, Felix Freiling, Anshul Gandhi, Rahul George, Kanad Ghose, Kartik Gopalan, Ryan Guide, Amy Hasan, Ting He, Blaine Hoak, Thorsten Holz, Syed Rafiul Hussain, Syed Rafiul Hussain, Alban Héon, Trent Jaeger, Somesh Jha, Rachel King, Engin Kirda, Farinaz Koushanfar, Srikanth V. Krishnamurthy, Daniel E. Krych, Domico, Kyle, Thomas La Porta, Dongyoon Lee, Kunyang Li, Azaree Lintereur, David Liu, David Yu Liu, Zhenhua Liu, Andrea Matwyshyn, Patrick McDaniel, Paul Barford Patrick McDaniel, Patrick Mcdaniel, Fidan Mehmeti, Shuai Mu, Namitha Nambiar, Michael Norris, Kyle Ostrowski, Nicolas Papernot, McDaniel, Patrick, Eric Pauley, Jonathan Petit, Jingyuan Qi, Burke, Quinn, Konrad Rieck,



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0114

Sheatsley, Ryan, Ahmad-Reza Sadeghi, Alejandro Andrade Salazar, Ryan Sheatsley, Tyler Shipp, Amit Kumar Sikder, Anand Sivasubramaniam, Wenjia Song, Indra Spiecker, Michael Swift, Gang Tan, Sanchal Thakkar, Selcuk Uluagac, Prasanna Venkatesh, Gunjan Verma, Bimal Viswanath, Michael J. Weisman, Ya Xiao, Tian Xie, Danfeng Yao, Beugin, Yohan, Mingi Yu, Mingli Yu, Erez Zadok, Danfeng Zhang, Shulin Zhao, Sencun Zhu, Shitong Zhu, Bolor-Erdene Zolbayarn

## CASES (Expert Witness)

*DivX, LLC v. Hulu, LLC and Netflix, Inc.*, Expert for Expert for the Defence, Central District of California, Case no. Case No. 2:19-cv-01602.

*Inter Partes Review*, Expert for Expert for Apple Inc., United States Patent and Trademark Office, Case no. Patent Nos. 9,947,000, 9,928,495 and 10,163,103.

*Trusted Knight Corporation v. International Business Machines Corporation*, Expert for Expert for IBM Corporation, Northern District of California, Case no. Case No. 3:19-cv-01206-EMC.

*Inter Partes Review*, Expert for Expert for IBM Coperation, United States Patent and Trademark Office, Case no. Patent No. 9,503,473.

*Finjan Inc., vs. Rapid7 Inc and Rapid7 LLC*, Expert for Expert for Rapid7, District of Deleware, Case no. C.A. No. 1:18-CV-01519-MN.

*Finjan Inc., vs. Cisco Systems, Inc.*, Expert for Expert for CISCO, Northern District of California, San Jose Division, Case no. Case No. 5:17-cv-00072-BLF-SVK.

*Inter Partes Review*, Expert for Expert forBlackBerry Limited, United States Patent and Trademark Office, Case no. Patent Nos. 8,825,084 and 8,326,327.

*BlackBerry Limited v. Snap. Inc.*, Expert for Expert for BlackBerry Limited, Central District of California, Case no. Case No. 2: 18-cv-02693.

*Rimini Street, Inc. v. Oracle International Corporation*, Expert for Expert for Oracle, United States District Court, District of Nevada, Case no. Case No. 2:14-cv-01699.

*Inter Partes Review*, Expert for Expert for Google Inc., United States Patent and Trademark Office, Case no. Patent No. 9,444,812.

*Good Technology Corporation et al., v. AirWatch, LLC*, Expert for Expert for Airwatch LLC, United States District Court for the Northern District of California, Case no. 5-12-cv-05827.

*Inter Partes Review*, Expert for Duo Security Inc., United States Patent and Trademark Office, Case no. IPR2017-01041.

*Inter Partes Review*, Expert for Duo Security Inc., United States Patent and Trademark Office, Case no. IPR2017-01064.

*Frederick Whalen, et al., v. SEI/AARON'S, INC.*, Expert for defense, United States District Court for the Northern District of Georgia, Case no. 1:2014-cv-01209.

*Certain Portable Electronic Communications Devices, Including Mobile Phones and Components Thereof*, Expert for plaintiff, International Trade Commission.

*Secure Axcess, LLC v. Bank of America Corp., et al.*, Expert for defense, United States District Court for the Eastern District of Texas, Tyler Division, Case no. 6-10-cv-00670.

*Intellectual Ventures I LLC, v. Check Point et al.*, Expert for plaintiff, United States District Court for the District of Delaware, Case no. 1-10-cv-01067.

*NetMonitor LLC, v. Compuware et al.*, Expert for plaintiff, United States District Court for the District of Delaware, Case no. 1-10-cv-01061.

*Amdocs Ltd. v. Openet Telcom Ltd.*, Expert for defense, United States District Court for the Eastern District of Virginia, Alexandria Division, Case no. 1-10-cv-00910.

*PSI Systems Inc. v. Stamps.com*, Expert for defense, United States District Court for the Central District of California, Case no. 2-08-cv-05233.

*Stamps.com v. Endicia*, Expert for plaintiff, United States District Court for the Central District of California, Case no. 2-06-cv-07499.

*Kara Technologies v. Stamps.com*, Expert for defense, United States District Court for the Central District of California, Case no. 2-05-cv-01890.

*Coinstar Inc. v. Coinxchange*, Expert for defense, United States District Court for the Eastern District of Virginia, Richmond Division, Case no. 3-06-cv-00299.

*VCode Holdings Inc. v. Stamps.com*, Expert for defense, United States District Court for the Central District of California.

*Inter Partes Review*, Expert for Google Inc.,, United States Patent and Trademark Office, Case no. (Patent No. 8,489,868).

*Inter Partes Review*, Expert for Cisco Systems, Inc., , Case no. (Patent No. 7,536,598).

*Vir2us v. Cisco Systems, INC and Sourcefire, LLC*, Expert for defense, United States District Court for the Eastern District of Virginia, Case no. 51:16cv1095.

*Zito Vault, LLC V. International Business Machines Corporation, and Softlayer Technologies, Inc.*, Expert for defense, , Case no. 3:16-CV-962-M.

## INDUSTRIAL EXPERIENCE

**Software Developer** 1994-1995
Applied Innovation, Inc., Columbus, OH

**Project Manager** 1993-1994
Primary Access Corporation, San Diego, CA

**Software Developer** 1991-1993
Primary Access Corporation, San Diego, CA

**Software Developer** 1989
Integrated Technologies, Inc., Muncie, IN

# PUBLICATIONS

## Books and Book Chapters

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *Security for Telecommunications Networks*, Springer, Advances in Information Security, July, 2008, ISBN: 978-0-387-72441-6.

Bolor-Erdene Zolbayar and Ryan Sheatsley and Patrick McDaniel, *Evading Machine Learning based Network Intrusion Detection Systems with GANs*, Game Theory and Machine Learning for Cyber Security, John Wiley & Sons, 2021. Eds. Charles A Kamhoua and Christopher D. Kiekintveld and Fei Fang and Quanyan Zhu. Hoboken, New Jersey.

Kevin Butler and William Enck and Patrick Traynor and Jennifer Plasterr and Patrick McDaniel, *Privacy Preserving Web-Based Email*, Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research, World Scientific Computing, 349-371, November, 2008. Eds. Bhargab Bhattacharya, Susmita Sur-Kolay, Subhas Nandy and Aditya Bagchi.

Patrick McDaniel, *Authentication*, Handbook of Computer Networks, Volume II, Chapter 171, John Wiley and Sons, May, 2007. Eds. Hossein Bidgoli.

Patrick McDaniel, *Computer and Network Authentication*, Handbook of Information Security, John Wiley and Sons, September, 2004. Eds. Hossein Bidgoli.

Patrick McDaniel, *IPsec*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Policy*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Authentication*, The Internet Encyclopedia, John Wiley and Sons, 2002.

## Journal Articles

Mingi Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *Stealthy Misreporting Attacks Against Load Balancing*, IEEE/ACM Transactions on Networking (TON), 2024.

Anshul Gandhi and Dongyoon Lee and Zhenhua Liu and Shuai Mu and Erez Zadok and Kanad Ghose and Kartik Gopalan and David Yu Liu and Syed Rafiul Hussain and Patrick McDaniel, *Metrics for Sustainability in Data Centers*, SIGENERGY Energy Inform. Rev., New York, NY, USA, ACM, 3, 3, 40–46, October, 2023.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2023.

Tian Xie and Sanchal Thakkar and Ting He and Patrick McDaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, IEEE Transactions on Parallel and Distributed Systems, May, 2023.

Ya Xiao and Wenjia Song and Jingyuan Qi and Bimal Viswanath and Patrick McDaniel and Danfeng Yao, *Specializing Neural Networks for Cryptographic Code Completion Applications*, IEEE Transactions on Software Engineering, IEEE, 2023.

Matthew Durbin and Ryan Sheatsley and Patrick McDaniel and Azaree Lintereur, *Experimental tests of Gamma-ray Localization Aided with Machine-learning (GLAM) capabilities*, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 1038, 2022.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *Who's Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment*, ACM Transactions on Internet of Things, Association for Comput-



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0117

ing Machinery, May, 2022.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Flexible Fault Handling in Diverse IoT Deployments*, ACM Transactions on Internet of Things, ACM, 2022.

Tian Xie and Namitha Nambiar and Ting He and Patrick McDaniel, *Attack Resilience of Cache Replacement Policies: A Study Based on TTL Approximation*, IEEE/ACM Transactions on Networking, 2022.

Quinn Burke and Fidan Mehmeti and Rahul George and Kyle Ostrowski and Trent Jaeger and Thomas La Porta and Patrick Mcdaniel, *Enforcing Multilevel Security Policies in Unstable Networks*, IEEE Transactions on Network and Service Management, IEEE, June, 2022.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples for Network Intrusion Detection Systems*, Journal of Computer Security (JCS), IOS Press, January, 2022.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2021.

Daniel E. Krych and Patrick McDaniel, *Exposing Android Social Applications: Linking Data Leakage to Privacy Policies*, Journal of Cyber Security Technology, Taylor & Francis, 5, 3-4, 2021.

Alejandro Andrade Salazar and Ryan Sheatsley and Jonathan Petit and Patrick McDaniel, *Physics-based Misbehavior Detection System for V2X Communications*, SAE International Journal of Connected and Automated Vehicles, SAE International, June, 2021.

Mingli Yu and Tian Xie and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE/ACM Transactions on Networking, 29, 6, 1063-6692, December, 2021.

Leonardo Babun and Kyle Denney and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives*, Computer Networks, 192, 19, June, 2021.

Ryan Sheatsley and Matthew Durbin and Azaree Lintereur and Patrick McDaniel, *Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations*, IEEE Sensors, 21, 8, April, 2021.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, IEEE Transactions on Network and Service Management, 18, 1, March, 2021.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *Preparing for the Age of Deepfakes and Disinformation*, Stanford HAI Policy Brief, 2020.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant Is the Turing Test in the Age of Sophisbots?*, IEEE Security & Privacy Magazine, 17, 64-71, Nov/Dec, 2019.

Z. Berkay Celik and Patrick McDaniel and Thomas Bowen, *Malware Modeling and Experimentation through Parameterized Behavior*, Journal of Defense Modeling and Simulation (JDMS), 15, 1, 31-48, 2017.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Opportunities and Challenges*, ACM Computing Surveys (CSUR), ACM, 42, 4, 2019.

Z. Berkay Celik and Patrick McDaniel and Gang Tan and Leonardo Babun and Selcuk Uluagac, *Verifying IoT Safety and Security in Physical Spaces*, IEEE Security & Privacy Magazine, IEEE, 17, 5, 30-37, 2019.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0118

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Catch Me if You Can: Malicious Co-Residency on the Cloud*, IEEE/ACM Transactions on Networking, 27, 2, April, 2019.

Ian Goodfellow and Patrick McDaniel and Nicolas Papernot, *Making machine learning robust against adversarial inputs*, Communications of the ACM, ACM, 61, 7, 56-6, June/July, 2018.

Dave Tian and Kevin Butler and Joseph Choi and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP/NDP From the Ground Up*, IEEE Transactions on Information Forensics and Security, 12, 9, 2131-2143, April, 2017.

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chada, *Deceiving Network Reconnaissance Unsing SDN-based Virtual Topologies*, IEEE Transactions on Network and Service Management, Special Issue on Advances in Management of Softwarized Networks, 14, 4, July, 2017.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Dawn of the Dead Domain: Measuring the Exploitation of Residual Trust in Domains*, IEEE Security & Privacy Magazine (Secure Systems issue column), April, 2017.

Patrick McDaniel and Nicolas Papernot and Z. Berkay Celik, *Machine Learning in Adversarial Settings*, IEEE Security & Privacy Magazine, 14, 3, May/June, 2016.

Patrick McDaniel and Ananthram Swami, *The Cyber Security Collaborative Research Alliance:Unifying Detection, Agility, and Risk in Mission-Oriented Cyber Decision Making*, CSIAC Journal, Army Research Laboratory (ARL) Cyber Science and Technology, 5, 1, January, 2017.

Damien Octeau and Daniel Luchaup and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation and its Application to Android Program Analysis*, IEEE Transactions on Software Engineering, 42, 11, 999-1014, 2016.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Security Outlook: Six Cyber Game Changers for the Next 15 Years*, IEEE Computer, 47, 12, 104-106, 2014.

Zhenfu Cao and Keqiu Li and Xu Li and Patrick McDaniel and Radha Poovendran and Guojun Wang and Yang Xiang, *Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems*, IEEE Transactions on Parallel and Distributed Systems, 25, 2, 279-28, 2014.

Patrick McDaniel and Brian Rivera and Ananthram Swami, *Toward a Science of Secure Environments*, IEEE Security & Privacy Magazine, 12, 4, July/August, 2014.

William Enck and Peter Gilbert and Seungyeop Han and Vasant Tendulkar and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, ACM Transactions on Computer Systems (TOCS), 32, 2, June, 2014.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Communications of the ACM, 57, 3, March, 2014.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Security and Communication Networks, 5, 6, 658-673, 2012.

Patrick McDaniel, *Bloatware Comes to the Smartphone*, IEEE Security & Privacy Magazine, 10, 4, July/August, 2011.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0119

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Web Content Attestation*, IEEE Transactions on Computers, 61, 5, 686–699, April, 2011.

Patrick McDaniel, *Data Provenance and Security*, IEEE Security & Privacy Magazine, 9, 3, March/April, 2011.

Joshua Schiffman and Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Network-based Root of Trust for Installation*, IEEE Security & Privacy Magazine, 40-48, Jan/Feb, 2011.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel, *New Security Architectures Based on Emerging Disk Functionality*, IEEE Security and Privacy Magazine, 8, 5, October, 2010.

Patrick McDaniel and William Enck, *Not So Great Expectations: Why Application Markets Haven't Failed Security*, IEEE Security & Privacy Magazine, 8, 5, 76–78, September/October, 2010.

Patrick Traynor and Chaitrali Amrutkar and Vikhyath Rao and Trent Jaeger and Patrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Journal of Security and Communication Networks (SCN), 4, 6, 719 – 726, June, 2011.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, *malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Journal of Security and Communication Networks (SCN), 2, 3, 102-113, March, 2010.

Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Brent Waters, *Secure Attribute-Based Systems*, Journal of Computer Security (JCS), 18, 5, 799–837, 2010.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, ACM Transactions on Information and System Security (TISSEC), 13, 26, 2010.

Kevin Butler and Toni Farley and Patrick McDaniel and J. Rexford, *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE, 2010, 1, 100-122, January, 2010.

Kevin Butler and Sunam Ryu and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, IEEE Transactions on Parallel and Distributed Systems (TPDS), 20, 12, 1803-1815, December, 2009.

Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE Security & Privacy Magazine (Secure Systems issue column), 7, 3, 75-77, May/June, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, IEEE/ACM Transactions on Networking (TON), 17, 1, 40-53, February, 2009.

William Enck and Machigar Ongtang and Patrick McDaniel, *Understanding Android Security*, IEEE Security & Privacy Magazine, 7, 1, 50–57, January/February, 2009.

William Enck and Thomas Moyer and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Yu-Wei Sung and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, IEEE Journal on Selected Areas in Communications (JSAC), 27, 3, 323-335, 2009.

Heesook Choi and William Enck and Jaesheung Shin and Patrick McDaniel and Thomas La Porta, *ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks*, Wireless Networks (WINET), ACM/Kluwer, 15, 4, 525-539, May, 2009.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0120

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Journal of Computer Security, 16, 6, 713-742, Febraury, 2009.

Patrick Traynor and Michael Chien and Scott Weaver and Boniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, ACM Transactions on Information and System Security (TISSEC), 11, 3, 2008.

Patrick McDaniel and Bashar Nuseibeh, *Guest Editorial: Special Issue on Software Engineering for Secure Systems*, IEEE Transactions on Software Engineering, 34, 1, 3–4, 2008.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol*, Computer Networks, Elsevier, 51, 15, 4322–4337, October, 2007.

Patrick McDaniel and Avi Rubin, *Guest Editoral: Special Issue on Web Security*, Computer Networks, Elsevier, 22, 2, 2005.

Patrick McDaniel and Atul Prakash, *Enforcing Provisioning and Authorization Policy in the Antigone System*, Journal of Computer Security, 14, 6, 483–511, November, 2006.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, ACM Transactions on Information and System Security (TISSEC), Association for Computing Machinery, 9, 3, 259-291, August, 2006.

Patrick McDaniel and William Aiello and Kevin Butler and JohnIoannidis, *Origin Authentication in Interdomain Routing*, Journal of Communication Networks, Elsevier, 50, 16, 2953-2980, November, 2006.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysisand Methods of Defense*, International Journal of Distributed Sensor Networks, 2, 3, 267-287, June, 2005.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Telecommunications Policy, 28, 8, 619-644, August, 2004.

## Conference Publications

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2024.

Blaine Hoak and Patrick McDaniel, *Explorations in Texture Learning*, 12th International Conference on Learning Representations, Tiny Papers Track (ICLR), May, 2024.

Tian Xie and Sanchal Thakkar and Ting He and Novella Bartolini and Patrick McDaniel, *Host-based Flow Table Size Inference in Multi-hop SDN*, Proceedings of the IEEE GLOBECOM, IEEE, December, 2023. Kuala Lumpur, Malaysia.

Eric Pauley and Paul Barford and Patrick McDaniel, *The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits Against Two Years of Zero-Days*, Proceedings of the ACM 2023 Internet Measurement Conference (IMC), October, 2023. Montreal, Canada. (**runner up-best paper award**)

Mingli Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *mMLSnet: Multilevel Security Network With Mobility*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2023. Boston, MA.

Ryan Guide and Eric Pauley and Yohan Beugin and Ryan Sheatsley and Patrick McDaniel, *Characterizing the Modification Space of Signature IDS Rules*, MILCOM 2023 - 2023 IEEE Military Communications Conference



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0121

(MILCOM), IEEE, October, 2023. Boston, MA.

Eric Pauley and Paul Barford Patrick McDaniel, *DScope: A Cloud-Native Internet Telescope*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023. Anaheim, CA.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Patrick McDaniel, *The Space of Adversarial Strategies*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023.

Eric Pauley and Gang Tan and Danfeng Zhang and Patrick McDaniel, *Performant Binary Fuzzing without Source Code using Static Instrumentation*, Conference on Communications and Network Security (CNS), IEEE, October, 2022.

Patrick McDaniel, *Keynote Address: Sustainability is a Security Problem (extended abstract)*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2022.

Kyle Domico and Ryan Sheatsley and Yohan Beugin and Quinn Burke and Patrick McDaniel, *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*, Machine Learning in Heliophysics (ML-Helio), AGU, November, 2022.

Tian Xie and Sanchal Thakkar and Ting He and Patrick Mcdaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, Proceedings of the International Conference on Distributed Computing Systems (ICDCS), July, 2022.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Building a Privacy-Preserving Smart Camera System*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2022.

Eric Pauley and Ryan Sheatsley and Blaine Hoak and Quinn Burke and Yohan Beugin and Patrick McDaniel, *Measuring and Mitigating the Risk of IP Reuse on Public Clouds*, 2022 IEEE Symposium on Security and Privacy (IEEE S&P), IEEE, May, 2022. San Francisco, CA.

Ahmed Abdou and Ryan Sheatsley and Yohan Beugin and Tyler Shipp and Patrick McDaniel, *HoneyModels: Machine Learning Honeypots*, Proceedings of the Military Communications Conference (MILCOM), IEE, November, 2021.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2021.

Tian Xie and Ting He and Patrick McDaniel and Namitha Nambiar, *Attack Resilience of Cache Replacement Policies*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, May, 2021.

Adrien Cosson and Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information*, In 6th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2021.

Matthew Durbin and Ryan Sheatlsey and Patrick McDaniel and Azaree Lintereur, *A Multi-Step Machine Learning Approach to Directional Gamma Ray Detection*, 2020 IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC), October, 2020.

Sayed M. Saghaian and Thomas La Porta and Simone Silvestri and Patrick McDaniel, *Improving Robustness of a Popular Probabilistic Clustering Algorithm Against Insider Attacks*, International Conference on Security and Privacy in Communication Networks (SecureComm 2020), EAI, October, 2020.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks in Software-Defined Networking*, International Conference on Security and Privacy in Communication Networks



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0122

(SecureComm 2020), EAI, October, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), ACM, July, 2020.

Mingli Yu and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE INFOCOM, IEEE Conference on Computer Communications, June, 2020. Beijing, China.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Systematically addressing device faults in commodity IoT*, In 5th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2020.

Raquel Alvarez and Jake Levenson and Ryan Sheatsley and Patrick McDaniel, *Application Transiency: Towards a Fair Trade of Personal Information for Application Services*, Proceedings of the EAI Conference on Security and Privacy in Communication Networks (SecureComm), October, 2019. Orlando, FL.

Giuseppe Petracca and Yuqiong Sun and Ahmad-Atamli Reineh and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *EnTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs*, Proceedings of the 28th USENIX Security Symposium, Augus, 2019. Santa Clara, CA.

Matthew Durbin and Ryan Sheatsley and Christopher Balbier and Tristan Grieve and Patrick McDaniel and Azaree Lintereur, *Development of Machine Learning Algorithms for Directional Gamma Ray Detection*, Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July, 2019. Palm Desert, CA. (**J. D. Williams student paper award, Nuclear Security and Physical Protection division**)

Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, ACM Conference on Data and Applications Security (CODASPY), March, 2019. Dallas, TX.

Z. Berkay Celik and Gang Tan and Patrick McDaniel, *IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT*, Network and Distributed System Security Symposium (NDSS), February, 2019. San Diego, CA.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '18), December, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Proceedings of the 27th USENIX Security Symposium, August, 2018. Baltimore, MD.

Rauf Izmailov and Shridatt Sugrim and Ritu Chadha and Patrick McDaniel and Ananthram Swami, *Enablers Of Adversarial Attacks in Machine Learning*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2018.

Sayed M. Saghaian and Thomas La Porta and Trent Jaeger and Z. Berkay Celik and Patrick McDaniel, *Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout*, Proceedings of EAI SECURECOMM 2018, August, 2018. (**best paper award**)

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, USENIX Annual Technical Conference (USENIX ATC), July, 2018. Boston, MA.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0123

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, ACM Asia Conference on Computer and Communications Security (ASIACCS), June, 2018.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, International Conference on Learning Representations (ICLR), 2018. Vancouver, Canada.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *SoK: Security and Privacy in Machine Learning*, Security and Privacy (EuroS&P), 2018 IEEE European Symposium on on Security and Privacy (EuroS&P), IEEE, April, 2018. London, UK.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, 13th IEEE International Conference on Network and Service Management, November, 2017. Tokyo, Japan.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Examples for Malware Detection*, 22nd European Symposium on Research in Computer Security (ESORICS '17), September, 2017. Oslo, Norway.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Cimplifier: Automatically Debloating Containers*, 11Th Joint Meeting of the European Software Engineering Conference and the Acm Sigsoft Symposium on the Foundations of Software Engineering, September, 2017. Paderborn, Germany.

Yunfeng Hong and Yongjian Hu and Chun-Ming Lai and Felix Wu and Iulian Neamtiu and Yu Paul and Patrick McDaniel and Hasan Cam and Gail-Joon Ahn, *Defining and Detecting Environment Discrimination in Android Apps*, The 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 17), October, 2017.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017, April, 2017.

Stefan Achleitner and Thomas La Porta and Trent Jaeger and Patrick McDaniel, *Adversarial Network Forensics in Software Defined Networking*, ACM Symposium on SDN Research (SOSR), ACM, April, 2017. (**best student paper award**)

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Srikanth V. Krishnamurthy and Alexander Poylisher and Constantin Serban, *Stealth Migration: Hiding Virtual Machines on the Network*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Malicious Co-Residency on the Cloud: Attacks and Defense*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Nathaniel Lageman and Eric Kilmer and Robert Walls and Patrick McDaniel, *BinDNN: Resilient Function Matching Using Deep Learning*, 2016 International Conference on Security and Privacy in Communication Networks (SECURECOMM), October, 2016.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0124

Z. Berkay Celik and Nan Hu and Yun Li and Nicolas Papernot and Patrick McDaniel and Jeff Rowe and Robert Walls and Karl Levitt and Novella Bartolini and Thomas La Porta and Ritu Chadha, *Mapping Sample Scenarios to Operational Models*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Michael Backes and Sven Bugiel and Erik Derr and Patrick McDaniel and Damien Octeau and Sebastian Weisgerber, *On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis*, Proceedings of the 25th USENIX Security Symposium, August, 2016.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2016.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Domain-Z: 28 Registrations Later*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Yasemin Acar and Michael Backes and Sven Bugiel and Sascha Fahl and Patrick McDaniel and Matthew Smith, *SoK: Lessons Learned From Android Security Research For Appified Software Platforms*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Charles Huber and Scott Brown and Patrick McDaniel and Lisa Marvel, *Cyber Fighter Associate: A Decision Support System for Cyber Agility*, Proceedings of the 50th Annual Conference on Information Sciences and Systems (CISS), March, 2016. Princeton, NJ.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Proceedings of the 1st IEEE European Symposium on Security and Privacy, IEEE, 2016. Saarbrucken, Germany.

Damien Octeau and Somesh Jha and Matthew Dering and Patrick McDaniel and Alexandre Bartel and Li Li and Jacques Klein and Yves Le Traon, *Combining Static Analysis with Probabilistic Models to Enable Market-Scale Android Inter-Component Analysis*, Proceedings of the 43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), January, 2016. St. Petersburg, Florida, USA.

Devin Pohly and Patrick McDaniel, *MICSS: A Realistic Multichannel Secrecy Protocol*, IEEE Global Communications Conference (GLOBECOM), December, 2015. San Diego, CA.

Robert Walls and Eric Kilmer and Nathaniel Lageman and Patrick McDaniel, *Measuring the Impact and Perception of Acceptable Advertisements*, Proceedings of the ACM 2015 Internet Measurement Conference (IMC), October, 2015. Tokyo, Japan.

Nicolas Papernot and Patrick McDaniel and Robert Walls, *Enforcing Agile Access Control Policies in Relational Databases using Views*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Computational Ontology of Network Operations*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Z. Berkay Celik and Robert Walls and Patrick McDaniel and Ananthram Swami, *Malware Traffic Detection using Tamper Resistant Features*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Devin Pohly and Charles Sestito and Patrick McDaniel, *Adaptive Protocol Switching Using Dynamically Insertable Bumps in the Stack*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Azeem Aqil and Ahmed Atya and Trent Jaeger and Srikanth V. Krishnamurthy and Karl Levitt and Patrick McDaniel and Jeff Rowe and Ananthram Swami, *Detection of Stealthy TCP-based DoS Attacks*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Daniel E. Krych and Stephen Lange-Maney and Patrick McDaniel and William Glodek, *Investigating Weaknesses in Android Certificate Security*, SPIE 9478, Modeling and Simulation for Defense Systems and Applications X, May, 2015.

Damien Octeau and Daniel Luchaup and Matthew Dering and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation: Application to Android Inter-Component Communication Analysis*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Li Li and Alexandre Bartel and Tegawende Bissyande and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Octeau and Patrick McDaniel, *IccTA: Detecting Inter-Component Privacy Leaks in Android Apps*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Jing Tian and Kevin Butler and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP From the Ground Up*, CODASPY '15: Proceedings of the 5th ACM Conference on Data Application and Security and Privacy, March, 2015. San Antonio, TX, USA.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Building an Ontology of Cyber Security*, Proc. Intl. Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS), November, 2014.

Matthew Dering and Patrick McDaniel, *Android Market Reconstruction and Analysis*, Proceedings of the Military Communications Conference (MILCOM), October, 2014. Baltimore, MD.

Wenhui Hu and Damien Octeau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), July, 2014. Oxford, United Kingdom.

Steven Arzt and Siegfried Rasthofer and Christian Fritz and Eric Bodden and Alexandre Bartel and Jacques Klein and Yves Le Traon and Damien Octeau and Patrick McDaniel, *FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps*, Proceedings of the 35th Conference on Programming Language Design and Implementation (PLDI), June, 2014. Edinburgh, UK.

Phillip Koshy and Diana Koshy and Patrick McDaniel, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, Proceedings of Financial Cryptography 2014, International Financial Cryptography Association (IFCA), February, 2014. Christ Church, Barbado.

Stephen McLaughlin and Devin Pohly and Patrick McDaniel and Saman Zonouz, *A Trusted Safety Verifier for Process Controller Code*, Proc. ISOC Network and Distributed Systems Security Symposium (NDSS), February, 2014. San Diego, CA.

Damien Octeau and Patrick McDaniel and Somesh Jha and Alexandre Bartel and Eric Bodden and Jacques Klein and Yves Le Traon, *Effective Inter-Component Communication Mapping in Android with Epicc: An Essential Step Towards Holistic Security Analysis*, Proceedings of the 22th USENIX Security Symposium, August, 2013.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0126

Washington, DC.

Devin J. Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), December, 2012. Orlando, Florida.

Stephen McLaughlin and Patrick McDaniel, *SABOT: Specification-based Payload Generation for Programmable Logic Controllers*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Weining Yang and Ninghui Li and Yuan Qi and Wahbeh Qardaji and Stephen McLaughlin and Patrick McDaniel, *Minimizing Private Data Disclosures in the Smart Grid*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Eun Kyoung Kim and Patrick McDaniel and Thomas La Porta, *A Detection Mechanism for SMS Flooding Attacks in Cellular Networks*, Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SECURECOMM 2012), September, 2012. Padua, Italy.

Damien Octeau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, 20th International Symposium on the Foundations of Software Engineering (FSE), November, 2012. Research Triangle Park, NC. (**best artifact award**)

Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Scalable Integrity-Guaranteed AJAX*, Proceedings of the 14th Asia-Pacific Web Conference (APWeb), April, 2012. Kunming, China. (*Invited Paper*)

Patrick McDaniel and Stephen McLaughlin, *Structured Security Testing in the Smartgrid*, Proceedings of 5th International Symposium on Communications, Control, and Signal Processing, May, 2012. Rome, Italy. (*Invited Paper*)

Stephen McLaughlin and Patrick McDaniel and William Aiello, *Protecting Consumer Privacy from Electric Load Monitoring*, The 18th ACM Conference on Computer and Communications Security (CCS), October, 2011. Chicago, IL.

William Enck and Damien Octeau and Patrick McDaniel and Swarat Chaudhuri, *A Study of Android Application Security*, Proceedings of the 20th USENIX Security Symposium, August, 2011. San Francisco, CA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, IEEE Global Communications Conference (GLOBECOM), December, 2010. Miami, FL.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October, 2010. Vancouver, BC.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0127

Toby Ehrenkranz and Jun Li and Patrick McDaniel, *Realizing A Source Authentic Internet*, Proceedings of the 6th International ICST Conference on Security and Privacy in Communications Networks (Securecomm), September, 2010. Singapore.

Boniface Hicks and Sandra Rueda and David King and Thomas Moyer and Joshua Schiffman and Yogesh Sreenivasan and Patrick McDaniel and Trent Jaeger, *An Architecture for Enforcing End-to-End Access Control over Web Applications*, Proceedings of the Fifteenth ACM Symposium on Access Control Models and Technologies (SACMAT 2010), 163-172, June, 2010. Pittsburgh, PA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Disk-Enabled Authenticated Encryption*, Proceedings of the 26th IEEE Symposium on Massive Storage Systems and Technologies (MSST), May, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 340-349, December, 2009. Honolulu, Hawaii. (**best paper**)

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 95-104, December, 2009. Honolulu, Hawaii.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 83-92, December, 2009. Honolulu, Hawai.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 235-245, November, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 223-234, November, 2009.

William Enck and Patrick McDaniel and Trent Jaeger, *PinUP: Pinning User Files to Known Applications*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

William Enck and Kevin Butler and Thomas Richardson and Patrick McDaniel and Adam Smith, *Defending Against Attacks on Main Memory Persistence*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), November, 2008. Alexandria, VA.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, ISOC Network & Distributed System Security Symposium (NDSS), February, 2008. San Diego, CA.

Luke St. Clair and Joshua Schiffman and Trent Jaeger and Patrick McDaniel, *Establishing and Sustaining System Integrity via Root of Trust Installation*, 23rd Annual Computer Security Applications Conference (ACSAC), 19-29, December, 2007. Miami, FL.

Boniface Hicks and Tim Misiak and Patrick McDaniel, *Channels: Runtime System Infrastructure for Security-typed Languages*, 23rd Annual Computer Security Applications Conference (ACSAC), 443-452, December, 2007. Miami, FL.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0128

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Proceedings of 2nd International Conference onInformation Systems Security (short paper), December, 2007. Delhi, India.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Fourth Conference on Email and Anti-Spam (CEAS 2007, August, 2007. Mountain View, California.

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *On Attack Causality in Internet-Connected Cellular Networks*, Proceedings of the 16th USENIX Security Symposium, 1–16, August, 2007. Boston, MA.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *From Trusted to Secure: Building and Executing Applications that Enforce System Security*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

William Enck and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS*, 12th ACM Symposium on Access Control Models andTechnologies (SACMAT), ACM, June, 2007. Sophia Antipolis, France.

Anusha Sriraman and Kevin Butler and Patrick McDaniel and Padma Raghavan, *Analysis of IPv4 Address Space Delegation Structure*, 12th IEEE Symposium on Computers and Communications (ISCC), July, 2007. Aveiro, Portugal.

Heesook Choi and Thomas La Porta and Patrick McDaniel, *Privacy Preserving Communication in MANETs*, Proceedings of Fourth Annual IEEE CommunicationsSociety Conference on Sensor, Mesh, and Ad Hoc Communications andNetworks (SECON 07), June, 2007. San Diego, CA.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Proceedings of 2007 IEEE International Conference onCommunications (ICC 2007), June, 2007. Glasgow, Scottlan.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node IDAssignment in Structured P2P Systems*, Proceedings of the 3rd IEEE International Symposium onSecurity in Networks and Distributed Systems (SSNDS-07), June, 2007. Niagra Falls, Canada.

Hosam Rowaihy and William Enck and Patrick McDaniel andThomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Proceedings of IEEE INFOCOM 2007 MiniSymposiu, May, 2007. Anchorage, AK.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *Understanding Practical Application Development in Security-Typed Languages*, 22st Annual Computer Security Applications Conference (ACSAC), 153–164, December, 2006. Miami, Fl. (**best student paper**)

Luke St. Clair and Lisa Johansen and William Enck and Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Trent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 37–55, December, 2006. Kolkata, India.

Kevin Butler and William Enck and Jennifer Plasterr and Patrick Traynor and Patrick McDaniel, *Privacy-Preserving Web-Based Email*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 116–131, December, 2006. Kolkata, India.

Matthew Pirretti and Patrick Traynor and PatrickMcDaniel and Brent Waters, *Secure Attribute-Based Systems*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 99-112, November, 2006. Alexandria, VA.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0129

Kevin Butler and William Aiello and Patrick McDaniel, *Optimizing BGP Security by Exploiting Path Stability*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 298-310, November, 2006. Alexandria, VA.

Patrick Traynor and William Enck and Patrick McDaniel andThomas La Porta, *Mitigating Attacks on Open Functionality in SMS-CapableCellular Networks*, Proceedings of the Twelfth Annual InternationalConference on Mobile Computing and Networking (MobiCom), 182-193, September, 2006. Los Angeles, CA.

Patrick Traynor and Michael Chien and Scott Weaver andBoniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Proceedings of the Second IEEE CommunicationsSociety/CreateNet International Conference on Security and Privacyin Communication Networks (SecureComm), August, 2006. Baltimore, MD.

Sophie Qiu and Patrick McDaniel and Fabian Monrose andAvi Rubin, *Characterizing Address Use Structure and Stabillity ofOrigin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, 489-496, June, 2006. Pula-Cagliari, Sardinia, Italy.

Patrick McDaniel and Shubho Sen and Oliver Spatscheck andJacobus Van der Merwe and William Aiello and Charles Kalmanek, *Enterprise Security: A Community of Interest Based Approach*, Proceedings of Network and Distributed Systems Security2006 (NDSS), February, 2006. San Diego, CA.

Kevin Butler and Patrick McDaniel, *Understanding Mutable Internet Pathogens, or How I Learnedto Stop Worrying and Love Parasitic Behavior*, Proceedings of 1st International Conference onInformation Systems Security (ICISS), Springer-Verlag Lecture Notes in Computer Science, volume 3803, 36-48, December, 2005. Kolkata, India. (*Invited Paper*)

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, 21st Annual Computer Security Applications Conference(ACSAC), 95-103, December, 2005. Tuscon, AZ.

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the 12th ACM Conference on Computer and CommunicationsSecurity (CCS), 393–404, May, 2005. Alexandria, VA.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysisand Methods of Defense*, Proceedings of the Innovations and CommercialApplications of Distributed Sensor Networks Symposi, October, 2005. Bethesda, Maryland. (**best paper**)

Louis Kruger and Somesh Jha and Patrick McDaniel, *Privacy Preserving Clustering*, 10th European Symposium on Research in ComputerSecurity (ESORICS '05), September, 2005. Milan, Italy.

Heesook Choi and William Enck and Jaesheung Shin andPatrick McDaniel and Thomas La Porta, *Secure Reporting of Traffic Forwarding Activity in Mobile AdHoc Networks*, MobiQuitous 2005, July, 2005. San Diego, CA.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDanie, *Exposing Digital Content Piracy: Approaches, Issues and Experiences*, Thirty-Eighth Conference on Signals, Systems, and Computers, 45–50, Nov, 2004. Monterey, CA. (*Invited paper*)

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Proceedings of 10th ACM Conference on Computer andCommunications Security (CCS), ACM, 165-178, October, 2003. Washington, DC.

Eric Cronin and Sugih Jamin and Tal Malkin and PatrickMcDaniel, *On the Performance, Feasibility, and Use of Forward SecureSignatures*, Proceedings of 10th ACM Conference on Computer andCommunications Security (CCS), ACM, 131-144, October, 2003. Washington, DC.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0130

Patrick McDaniel, *On Context in Authorization Policy*, 8th ACM Symposium on Access Control Models andTechnologies (SACMAT), ACM, 80-8, June, 2003. Como, Italy.

Geoff Goodell and William Aiello and Tim Griffin and John Ioannidis and Patrick McDaniel and Avi Rubin, *Working Around BGP: An Incremental Approach to ImprovingSecurity and Accuracy of Interdomain Routing*, Proceedings of Network and Distributed Systems Security2003 (NDSS), Internet Society, 75-8, February, 2003. San Diego, CA.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, 2002 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 73-87, May, 2002. Oakland, CA.

Patrick McDaniel and Atul Prakash and Jim Irrer and Sharad Mittal and Thai-Chuin Thuang, *Flexibly Constructing Secure Groups in Antigone 2.0*, Proceedings of DARPA Information SurvivabilityConference and Exposition II, IEEE Computer Society Press, 55-67, June, 2001. Los Angeles, CA.

Hugh Harney and Andrea Colegrove and Patrick McDaniel, *Principles of Policy in Secure Groups*, Proceedings of Network and Distributed Systems Security2001 (NDSS), Internet Society, 125-13, February, 2001. San Diego, CA.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Proceedings of IEEE INFOCOM 2000, IEEE, 1406-1414, March, 2000. Tel Aviv, Israel.

Patrick McDaniel and Avi Rubin, *A Response to 'Can We Eliminate Certificate RevocationLists?'*, Proceedings of Financial Cryptography 2000, International Financial Cryptography Association(IFCA), February, 2000. Anguilla, British West Indies.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman andPatrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing*, Proceedings of Communications and Multimedia Security(CMS '99), 176-190, September, 1999. Katholieke Universiteit, Leuven, Belgium.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Proceedings of the 8th USENIX Security Symposium, 99-114, August, 1999. Washington, DC.

## Workshop Papers

Yohan Beugin and Patrick McDaniel, *A Public and Reproducible Assessment of the Topics API on Real Data*, SecWeb 2024 Workshop, IEEE Security and Privacy Workshops (SPW), May, 2024.

Kunyang Li and Kyle D Domico and Jean-Charles Noirot Ferrand and Patrick McDaniel, *The Efficacy of Transformer-Based Adversarial Attacks in Security Domains*, Workshop on Artificial Intelligence for Cyber (MILCOM 2023, October, 2023. Boston, MA.

Eric Pauley and Patrick McDaniel, *Understanding the Ethical Frameworks of Internet Measurement Studies*, The 2nd International Workshop on Ethics in Computer Security (EthiCS 2023), February, 2023. San Diego, CA. (**best paper award**)

Anshul Gandhi and Kanad Ghose and Kartik Gopalan and Syed Rafiul Hussain and Dongyoon Lee and David Liu and Zhenhua Liu and Patrick McDaniel and Shuai Mu and Erez Zadok, *Metrics for Sustainability in Data Centers*, Proceedings of the 1st Workshop on Sustainable Computer Systems Design and Implementation (HotCarbon'22), USENIX, July, 2022. San Diego, CA.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Privacy Enhancing Technologies Symposium (PETS), 2021.

Sushrut Shringarputale and Patrick McDaniel and Kevin Butler and Thomas La Porta, *Co-residency Attacks on Containers are Real*, The ACM Cloud Computing Security Workshop (CCSW 2020), 2020.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0131

Z. Berkay Celik and Patrick McDaniel, *Extending Detection with Privileged Information via Generalized Distillation*, IEEE Security & Privacy Workshop on Deep Learning and Security (IEEE S&P DLS), 2018.

Alexander Alexeev and Diane Henshel and Karl Levitt and Patrick McDaniel and Brian Rivera and Steve Templeton and Michael J. Weisma, *Constructing a Science of Cyber-Resilience for Military Systems*, Information Systems and Technology (IST) Panel, IST-153/RWS-21, CEUR Workshop Proceeding, 30-42, October, 2017.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov, *Feature Cultivation in Privileged Information-augmented Detection*, Proceedings of the International Workshop on Security And Privacy Analytics (IWSPA 2017), 2017. (*Invited Paper*)

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chadha, *Cyber Deception: Virtual Networks to Defend Insider Reconnaissance*, Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, ACM, 2016.

Patrick McDaniel and Robert Walls, *Estimating Attack Intent and Mission Impact from Detection Signals*, Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks, Army Research Laboratory, July, 2015.

Patrick McDaniel and Trent Jaeger and Thomas La Porta and Nicolas Papernot and Robert Walls and Alexander Kott and Lisa Marvel and Ananthram Swami and Prasant Mohapatra and Srikanth V. Krishnamurthy and Iulian Neamtiu, *Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), November, 2014. Scottsdale, AZ.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Proccedings of CCSW 2010: The ACM Cloud Computing Security Workshop, October, 2010. Chicago, IL.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Embedded Firmware Diversity for Smart Electric Meters*, Proceedings of the 5th Workshop on Hot Topics inSecurity (HotSec '10), August, 2010. Washington, DC.

Patrick McDaniel and Kevin Butler and Stephen McLaughlin and Radu Sion and Erez Zadok and Marianne Winslett, *Towards a Secure and Efficient System for End-to-End Provenance*, the 2nd USENIX Workshop on the Theory and Practice of Provenance, February, 2010. San Jose, CA.

Thomas La Porta and Patrick McDaniel and Karl Rauscher and Jun Shu, *The Impact of Supply Chain on Information and Communications Technology Security*, In the 1st Workshop on Workshop on Telecommunications Infrastructure Protection and Security, December, 2009. Honolulu, Hawaii.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, In the 4th International Workshop on Critical Information Infrastructure Security, September, 2009. Bonn, Germany.

Matthew Blaze and Patrick McDaniel, *Below the Salt: The Dangers of Unfulfilled Physical Media Assumptions*, In Proceedings of Seventeenth International Workshop on Security Protocols, April, 2009. Cambridge, England.

Kevin Butler and William Enck and Harri Hursti and StephenMcLaughlin and Patrick Traynor and Patrick McDaniel, *Systemic Issues in the Hart InterCivic and Premier VotingSystems: Reflections Following Project EVEREST*, In Proceedings of the 3rd USENIX/ACCURATE ElectronicVoting Technology Workshop (EVT '08), July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007.

Alexandria, VA.

William Enck and Sandra Rueda and Yogesh Sreenivasan and JoshuaSchiffman and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users from "Themselves"*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007. Alexandria, VA.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Applications*, Proceedings of the 2nd ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS '07), ACM Press, June, 2007. San Diego, CA.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integration of SELinux and Security-typed Languages*, Proceedings of the 2007 Security-Enhanced Linux Workshop, March, 2007. Baltimore, MD.

Sophie Qiu and Fabian Monrose and Andreas Terzis and Patrick McDaniel, *Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing*, Proceedings of The Second Workshop on Secure Network Protocols (NPSec), November, 2006. Santa Barbara.

Shiva Chaitanya and Kevin Butler and Patrick McDaniel andAnand Sivasubramaniam, *Design, Implementation and Evaluation of Security iniSCSI-based Network Storage Systems*, Proceedings of 2nd International Workshop on StorageSecurity and Survivability (StorageSS 2006), October, 2006. Alexandria, Virginia.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and RamonCaceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Proceedings of the First Workshop on Hot Topics inSecurity (HotSec '06), July, 2006. Vancouver, B.C., Canada.

Kevin Butler and Patrick McDaniel and Sophie Qiu, *BGPRV: A Library for Fast and Efficient Routing Data Manipulation*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Kevin Butler and Patrick McDaniel, *Testing Large Scale BGP Security in Replayable NetworkEnvironments*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level Policy for aSecurity-Typed Language*, Proceedings of ACM SIGPLAN Workshop on ProgrammingLanguages and Analysis for Security, 65-74, June, 2006. Ottawa, Canada.

Ali Al-Lawati and Dongwon Lee and Patrick McDaniel, *Blocking in Private Information Matching*, Proceedings of Second International ACM SIGMOD Workshopon Information Quality in Information Systems, June, 2005. Baltimore, MD.

William Aiello and Charles Kalmanek and Patrick McDaniel andShubho Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Analysis of Communities Of Interest in Data Networks*, Passive and Active Measurement Workshop 2005, March, 2005. Boston, M.

Simon Byers and Lorrie Cranor and David Kormann andPatrick McDaniel, *Searching for Privacy: Design and Implementation of aP3P-Enabled Search Engine*, Proceedings of 2004 Workshop on Privacy EnhancingTechnologies (PETS), May, 2004. Toronto, Canad.

Hao Wang and Somesh Jha and Patrick McDaniel and MironLivn, *Security Policy Reconciliation in Distributed ComputingEnvironments*, Proceedings of 5th International Workshop on Policiesfor Distributed Systems and Networks (Policy 2004), IEEE Computer Society Press, 137-146, June, 2004. Yorktown Heights, N.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Proceedings of 2003 ACM Workshop on Digital RightsManagement, ACM, October, 2003. Washington, DC, also appeared in Telecommunications PolicyResearch Conference – September 2003.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0133

## Patents

U.S. Patent No. 7,873,350, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, January, 2011.

U.S. Patent No. 7,975,044, Oliver Spatscheck and Subhabrata Sen and Jacobus Van der Merwe and Patrick McDaniel, *Automated disambiguation of fixed-serverport-based applications from ephemeral applications*, July, 2011.

U.S. Patent No. 8,175,580, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, May, 2012.

U.S. Patent No. 8,453,227, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, May, 2013.

U.S. Patent No. 8,732,293, Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *System and method for tracking individuals on a data network using communities of interest*, May, 2014.

U.S. Patent No. 8,813,213, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, August, 2014.

## Other Publications

Patrick McDaniel and Farinaz Koushanfar, *NSF Secure and Trustworthy Computing 2.0 Vision Statement*, Public Report, August, 2023.

Patrick McDaniel and Thorsten Holz and Indra Spiecker and Genannt Dohmann and Christopher Burchard and Ahmad-Reza Sadeghi and Konrad Rieck and Kamalika Chaudhuri and Somesh Jha and Andrea Matwyshyn and David Evans and Felix Freiling and Amy Hasan, *Cybersecurity and Machine Learning: Vision Document, Report on the joint NSF/DFG Cybersecurity and Machine Learning Research Workshop*, Public Report, National Science Foundation/Deutsche Forschungsgemeinschaf, December, 2021.

Patrick McDaniel and John Launchbury, *Artificial Intelligence and Cybersecurity: Opportunities and Challenges 2019 Technical Workshop Report*, Public Report, Networking and Information Technology Research and Development Subcommittee, Machine Learning and Artificial Intelligence Subcommittee, and the Special Cyber Operations Research and Engineering Subcommittee of the National Science and Technology Council, 2020.

Patrick McDaniel and Avi Rubin, *Conference Proceedings*, 2008 IEEE Symposium on Security and Privacy, IEEE, May, 2008. Oakland, CA.

Patrick McDaniel and Kevin Butler and William Enck and Harri Hursti and Stephen McLaughlin and Patrick Traynor and Matthew Blaze and Adam Aviv and Pavol Cerny and Sandy Clark and Eric Cronin and Gaurav Shah and Micah Sherr and Giovanni Vigna and Richard Kemmerer and David Balzarotti and Greg Banks and Marco Cova and Viktoria Felmetsger and William Robertson and Fredrik Valeur and Joseph Lorenzo Hall and Laura Quilter, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, Ohio Secretary of State, Public Report, 2007.

Patrick McDaniel and Shyam K. Gupta, *Conference Proceedings*, The Third International Conference Information Systems Security, Springer, December, 2007. Delhi, India.

Birgit Pfitzmann and Patrick McDaniel, *Conference Proceedings*, 2007 IEEE Symposium on Security and Privacy, IEEE, May, 2007. Oakland, CA.

Patrick McDaniel, *Conference Proceedings*, The 14th USENIX Security Symposium, USENIX, August, 2005.

Baltimore, MD.

Patrick McDaniel, *Policy Evolution: Autonomic Environmental Security*, Software Engineering Research Center Showcase, USA, December, 2004.

Hugh Harney and Uri Meth and Andrea Colegrove and AngelaSchuett and Patrick McDaniel and Gavin Kenny and HaithamCruickshank and Sunil Iyengar, *GSAKMP (Draft)*, Internet Research Task Force, August, 2003.

Patrick McDaniel and Atul Prakash, *A Flexible Architecture for Security Policy Enforcement*, Proceedings of DARPA Information SurvivabilityConference and Exposition III, Research Summaries, 234-239, April, 2003.

Jim Irrer and Atul Prakash and Patrick McDaniel, *Antigone: Policy-Based Secure Group Communications Systems and AMirD: Antigone-Based Secure File Mirroring System*, Proceedings of DARPA Information SurvivabilityConference and Exposition III, Demo Summaries, 44-4, April, 2003.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, NASA Tech Briefs, 55, August, 2002.

Patrick McDaniel and Atul Prakash, *Antigone Secure Group Communication System*, NASA Tech Briefs, 2001.

Patrick McDaniel, *Policy Management in Secure Group Communication*, PhD Thesis, University of Michigan, Ann Arbor, MI, August, 2001.

Patrick McDaniel and Hugh Harney and Andrea Colegrove andAtul Prakash and Peter Dinsmore, *Multicast Security Policy Requirements and Building Blocks(Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), November, 2000.

Tom Hardjono and Hugh Harney and Patrick McDaniel and Andrea Colegroveand Peter Dinsmore, *Group Security Policy Token (Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), November, 2001.

Patrick McDaniel and Hugh Harney and Peter Dinsmore and Atul Prakash, *Multicast Security Policy (Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), June, 2000.

Patrick McDaniel, *8th USENIX Security Symposium Conference Summaries,Potpourri Session*, USENIX Login Magazine, 9-12, November, 1999.

Patrick McDaniel, *The Analysis of $D_i$, a Detailed Design Metric on LargeScale Software*, Masters Thesis, Ball State University, Muncie, IN, June, 1991.

## Technical Reports

Quinn Burke and Ryan Sheatsley and Rachel King and Michael Swift and Patrick McDaniel, *Cloud Storage Integrity at Scale: A Case for Dynamic Hash Trees*, Technical Report 2405.03830, arXiv preprint, May, 2024.

Alban Héon and Ryan Sheatsley and Quinn Burke and Blaine Hoak and Eric Pauley and Yohan Beugin and Patrick McDaniel, *Systematic Evaluation of Geolocation Privacy Mechanisms*, Technical Report 2309.06263, arXiv preprint, September, 2023.

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (Not Preserving)*, Technical Report 2306.03825, arXiv preprint, May, 2023.

Quinn Burke and Yohan Beugin and Blaine Hoak and Rachel King and Eric Pauley and Ryan Sheatsley and Mingli Yu and Ting He and Thomas La Porta and Patrick McDaniel, *Securing Cloud File Systems using Shielded Execution*, Technical Report 2305.18639, arXiv preprint, May, 2023.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0135

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Privacy-Preserving Protocols for Smart Cameras and Other IoT Devices*, Technical Report 2208.09776, arXiv preprint, August, 2022.

Pauley, Eric and Domico, Kyle and Hoak, Blaine and Sheatsley, Ryan and Burke, Quinn and Beugin, Yohan and McDaniel, Patrick, *EIPSIM: Modeling Secure IP Address Allocation at Cloud Scale*, Technical Report arXiv:2210.14999, arXiv preprint, 2022.

Bolor-Erdene Zolbayarn and Ryan Sheatsley and Patrick McDaniel and Michael J. Weisman and Sencun Zhu and Shitong Zhu and Srikanth V. Krishnamurthy, *Generating Practical Adversarial Network Traffic Flows using NIDSGAN*, Technical Report arXiv:2203.06694, arXiv preprint, March, 2022.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Technical Report arXiv:2105.08619, arXiv preprint, 2021.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples in Constrained Domains*, Technical Report arXiv:2011.01183, arXiv preprint, 2020.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, Technical Report INSR-500-TR-0500-2019, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2019.

Michael Norris and Z. Berkay Celik and Patrick McDaniel and Gang Tan and Prasanna Venkatesh and Shulin Zhao and Anand Sivasubramaniam, *IoTRepair: Systematically Addressing Device Faults in Commodity IoT (Extended Paper)*, Technical Report arXiv:2002.07641, arXiv preprint, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, Technical Report arXiv:1911.10186, arXiv preprint, 2020.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Technical Report arXiv:1911.10461, arXiv preprint, 2019.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant is the Turing Test in the Age of Sophisbots?*, Technical Report arXiv:1909.00056, arXiv preprint, 2019.

Chun-Ming Lai and Xiaoyun Wang and Jon W. Chapman and Yu-Cheng Lin and Yu-Chang Ho and Felix Wu and Patrick McDaniel and Hasan Cam, *More or Less? Predict the Social Influence of Malicious URLs on Social Media*, Technical Report arXiv:1812.02978, arXiv preprint, 2018.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Technical Report arXiv:1810.09551, arXiv preprint, 2018.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities*, Technical Report arXiv:1809.06962, arXiv preprint, 2018.

Giuseppe Petracca and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *Regulating Access to System Sensors in Cooperating Programs*, Technical Report arXiv:1808.05579, arXiv preprint, 2018.

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, Technical Report arXiv:1805.08876, arXiv preprint, 2018.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0136

Nicolas Papernot and Patrick McDaniel, *Deep k-Nearest Neighbors: Towards Confident, Interpretable and Robust Deep Learning*, Technical Report arXiv:1803.04765, arXiv preprint, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Technical Report arXiv:1802.08307, arXiv preprint, 2018.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, Technical Report arXiv:1802.04500, arXiv preprint, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Technical Report arXiv:1707.01871, arXiv preprint, 2017.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, Technical Report arXiv:1705.07204, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel, *Extending Defensive Distillation*, Technical Report arXiv:1705.05264, arXiv preprint, 2017.

Florian Tramer and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *The Space of Transferable Adversarial Examples*, Technical Report arXiv:1704.03453, arXiv preprint, 2017.

Z. Berkay Celik and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, Technical Report arXiv:1702.08342, arXiv preprint, 2017.

Kathrin Grosse and Praveen Manoharan and Nicolas Papernot and Michael Backes and Patrick McDaniel, *On the (Statistical) Detection of Adversarial Examples*, Technical Report arXiv:1702.06280, arXiv preprint, 2017.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Technical Report arXiv:1611.08648, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *Towards the Science of Security and Privacy in Machine Learning*, Technical Report arXiv:1611.03814, arXiv preprint, 2016.

Nicolas Papernot and Ian Goodfellow and Ryan Sheatsley and Reuben Feinman and Patrick McDaniel, *cleverhans v1.0.0: an adversarial machine learning library*, Technical Report arXiv:1610.0076, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel, *On the Effectiveness of Defensive Distillation*, Technical Report arXiv:1607.05113, arXiv preprint, 2016.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Perturbations Against Deep Neural Networks for Malware Classification*, Technical Report arXiv:1606.04435, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow, *Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples*, Technical Report arXiv:1605.07277, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Technical Report arXiv:1604.08275, arXiv preprint, 2016.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, Technical Report arXiv:1603.09638,



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0137

arXiv preprint, 2016.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Towards Least Privilege Containers with Cimplifier*, Technical Report arXiv:1602.08410, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, Technical Report arXiv:1602.02697, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report arXiv:1511.07528, arXiv preprint, 2015.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks*, Technical Report arXiv:1511.04508, arXiv preprint, 2015.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Six Potential Game-Changers in Cyber Security: Towards Priorities in Cyber Science and Engineering*, Technical Report arXiv:1511.00509, arXiv preprint, 2015.

Li Li and Alexandre Bartel and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Octeau and Patrick McDaniel, *I know what leaked in your pocket: uncovering privacy leaks on Android Apps with Static Taint Analysis*, Technical Report arXiv:1404.7431, arXiv preprint, 2014.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, Technical Report NAS-TR-0188-2016, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2016.

Wenhui Hu and Damien Octeau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2016.

Devin Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Technical Report NAS-TR-0160-2012, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2016.

Damien Octeau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, Technical Report NAS-TR-0150-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2011.

Stephen McLaughlin and Patrick McDaniel, *Protecting Consumer Privacy from Electric Load Monitoring*, Technical Report NAS-TR-0147-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2011.

William Enck and Patrick McDaniel, *Federated Information Flow Control for Mobile Phones*, Technical Report NAS-TR-0136-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2010.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Technical Report NAS-TR-0134-2010, Network and Security Research Center, Department of Computer Science



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0138

and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0133-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android* , Technical Report NAS-TR-0132-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Technical Report NAS-TR-0127-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Technical Report NAS-TR-0120-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2010.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Technical Report NAS-TR-0119-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Technical Report NAS-TR-0116-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0115-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Firma: Disk-Based Foundations for Trusted Operating Systems*, Technical Report NAS-TR-0114-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Technical Report NAS-TR-0113-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0110-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2010.

Boniface Hicks and Sandra Rueda and Yogesh Sreenivasan and Guruprasad Jakka and David King and Trent Jaeger and Patrick McDaniel, *An Architecture for Enforcing End-to-End Security Over Web Applications*, Technical Report NAS-TR-0104-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2009.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *No Node Is an Island: Shamon Integrity Monitoring Approach*, Technical Report NAS-TR-0103-2009, Network and Security



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0139

Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0099-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, Novemeber, 2008.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel and Trent Jaeger, *SwitchBlade: Policy-Driven Disk Segmentation*, Technical Report NAS-TR-0098-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2008.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Technical Report NAS-TR-0095-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, September, 2008.

William Enck and Machigar Ongtang and Patrick McDaniel, *Automated Cellphone Application Certification in Android (or) Mitigating Phone Software Misuse Before It Happens*, Technical Report NAS-TR-0094-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, September, 2008.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, Technical Report NAS-TR-0091-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Technical Report NAS-TR-0089-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, April, 2008.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, Technical Report NAS-TR-0084-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, December, 2007.

Stephen McLaughlin and Kevin Butler and William Enck and Patrick McDaniel, *Genbd - A Generic Block Device*, Technical Report NAS-TR-0082-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, November, 2007.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Technical Report NAS-TR-0074-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, June, 2007.

William Enck and Sandra Rueda and Joshua Schiffman and Yogesh Sreenivasan and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users From "Themselves"*, Technical Report NAS-TR-0073-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, June, 2007.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Technical Report NAS-TR-0071-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennslyvania State University, University Park, PA, USA, May, 2007.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, Technical Report NAS-TR-0070-2007, Network



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0140

and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, May, 2007.

Luke St. Clair and Joshua Schiffman and Trent Jaeger andPatrick McDaniel, *Establishing and Sustaining System Integrity viaRoot of Trust Installation*, Technical Report NAS-TR-0067-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennslyvania State University, University Park, PA, USA, April, 2007.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Language*, Technical Report NAS-TR-0065-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, April, 2007.

William Enck and Patrick McDaniel and Trent Jaeger, *Protecting User Files by Reducing Application Access*, Technical Report NAS-TR-0063-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *A Logical Specification and Analysis for SELinux MLSPolicy*, Technical Report NAS-TR-0058-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *From Trusted to Secure: Building and ExecutingApplications that Enforce System Security*, Technical Report NAS-TR-0061-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Lisa Johansen and Kevin Butler and William Enck andPatrick Traynor and Patrick McDaniel, *Grains of SANs: Building Storage Area Networks fromMemory Spots*, Technical Report NAS-TR-0060-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Patrick Traynor and Vikhyath Rao and Trent Jaeger andPatrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Technical Report NAS-TR-0059-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Anusha Sriraman and Kevin Butler and Patrick McDaniel andPadma Raghavan, *Analysis of the IPv4 Address Space Delegation Structure*, Technical Report NAS-TR-0057-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, December, 2006.

Luke St. Clair and Joshua Schiffman and Trent Jaeger andPatrick McDaniel, *Sum of the Parts: Composing Trust from Validation Primitives*, Technical Report NAS-TR-0056-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, November, 2006.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Technical Report NAS-TR-0054-2006, Network and Security Research Center, Department of Computer Science and Engineeering, Pennsylvania State University, University Park, PA, USA, October, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integrating SELinux with Security-typed Languages*, Technical Report NAS-TR-0052-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, October, 2006.

Patrick Traynor and William Enck and Patrick McDaniel andThomas La Porta, *Mitigating Attacks on Open Functionality in SMS-CapableNetworks*, Technical Report NAS-TR-0051-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA,



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0141

USA, October, 2006.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, malnets*: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Technical Report NAS-TR-0048-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *Breaking Down the Walls of Mutual Distrust: Security-typed Email Using Labeled IPsec*, Technical Report NAS-TR-0049-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, Technical Report NAS-TR-0043-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol (extended version)*, Technical Report NAS-TR-0046-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Patrick McDaniel, *Understanding Equivalance in High-Level and Information Flow Policy*, Technical Report NAS-TR-0042-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2006.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and Ramon Caceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Technical Report RC239664 (W0605-129), IBM Research Division, Yorktown Heights, NY, May, 2006.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Technical Report NAS-TR-0040-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, May, 2006.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *From Languages to Systems: Understanding PracticalApplication Development in Security-typed Languages*, Technical Report NAS-TR-0035-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, April, 2006.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level policy for asecurity-typed language*, Technical Report NAS-TR-0033-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, March, 2006.

Matthew Pirretti and Patrick Traynor and PatrickMcDaniel and Brent Waters, *Secure Attribute-Based Systems*, Technical Report NAS-TR-0028-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, February, 2006.

William Enck and Kevin Butler and Thomas Richardson andPatrick McDaniel, *Securing Non-Volatile Main Memory*, Technical Report NAS-TR-0029-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, February, 2006.

Luke St. Clair and Lisa Johansen and William Enck andMatthew Pirretti and Patrick Traynor and Patrick McDaniel andTrent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Technical Report NAS-TR-0030-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2006.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0142

Heesook Choi and Patrick McDaniel and Thomas La Porta, *Privacy Preserving Communication in MANETs*, Technical Report NAS-TR-0031-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December, 2005.

Matthew Pirretti and Vijaykrishnan Narayanan and PatrickMcDaniel and Bharat Madan, *SLAT: Secure Localization with Attack Tolerance*, Technical Report NAS-TR-0024-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, August, 2005.

Patrick Traynor and Michael Chien and Scott Weaver andBoniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Technical Report NAS-TR-0025-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, September, 2005.

Sophie Qiu and Patrick McDaniel and Fabian Monrose andAvi Rubin, *Characterizing Address Use Structure and Stabillity ofOrigin Advertizement in Interdomain Routing*, Technical Report NAS-TR-0018-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Hosam Rowaihy and William Enck and Patrick McDaniel andThomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Technical Report NAS-TR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Boniface Hicks and Patrick McDaniel and Ali Hurson, *Information Flow Control in Database Security: A CaseStudy for Secure Programming with Jif*, Technical Report NAS-TR-0011-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, Uni versity Park, PA, USA, April, 2005.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, Technical Report NAS-TR-0010-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

Patrick Traynor and Kevin Butler and William Enck andJennifer Plasterr and Scott Weaver and John van Bramer and PatrickMcDaniel, *Privacy-Preserving Web-Based Email*, Technical Report NAS-TR-0009-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Technical Report NAS-TR-0007-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, May, 2005.

Boniface Hicks and David King and Patrick McDaniel, *Declassification with Cryptographic Functions in aSecurity-Typed Language*, Technical Report NAS-TR-0004-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, January, 2005.

William Aiello and Kevin Butler and Patrick McDaniel, *Path Authentication in Interdomain Routing*, Technical Report TR NAS-TR-0002-2004, Network and Security Center, Department of Computer Science and Engineering, Penn State University, November, 2004.

Dan Pei and William Aiello and Anna Gilbert and PatrickMcDaniel, *Origin Disturbances in BGP*, Technical Report TD-62TJJF8, AT&T Labs - Research, Florham Park, NJ, July, 2004.

Kevin Butler and Toni Farley and Patrick McDaniel andJennifer Rexford, *A Survey of BGP Security Issues and Solutions*, Technical Report TD-5UGJ33, AT&T Labs - Research, Florham Park, NJ, February, 2004.

Patrick McDaniel and Atul Prakash, *Securing Distributed Applications Using a Policy-based Approach*, Technical Report TD-5UDKVD, AT&T Labs - Research, Florham Park, NJ, December, 2003.

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Technical Report TD-5QHG2G, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Eric Cronin and Sugih Jamin and Tal Malkin and PatrickMcDaniel, *On the Performance, Feasibility, and Use of Forward SecureSignatures*, Technical Report TD-5QHGBK, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Technical Report TD-5N6SJ4, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Patrick McDaniel, *On Context in Authorization Policy*, Technical Report TD-5JCJCK, AT&T Labs - Research, Florham Park, NJ, January, 2003.

Patrick McDaniel and Atul Prakash, *An Architecture for Security Policy Enforcement*, Technical Report TD-5C6JFV, AT&T Labs - Research, Florham Park, NJ, July, 2002.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, Technical Report TD57-PAW, AT&T Labs - Research, Florham Park, NJ, February, 2002.

Patrick McDaniel and Atul Prakash, *Ismene: Provisioning and Policy Reconciliation in SecureGroup Communication*, Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, Universityof Michigan, December, 2000.

Patrick McDaniel and Atul Prakash, *Lightweight Failure Detection in Secure GroupCommunication*, Technical Report CSE-TR-428-00, Electrical Engineering and Computer Science, Universityof Michigan, June, 2000.

Patrick McDaniel and Atul Prakash, *Antigone: Implementing Policy in Secure GroupCommunication*, Technical Report CSE-TR-426-00, Electrical Engineering and Computer Science, Universityof Michigan, May, 2000.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Technical Report CSE-TR-413-99, Electrical Engineering and Computer Science, Universityof Michigan, November, 1999.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Technical Report 99-2, Center for Information Technology Integration, September, 1999.

Patrick McDaniel and Avi Rubin, *A Response to "Can We Eliminate Certificate RevocationLists?"*, Technical Report 99.8.1, AT&T Labs - Research, Florham Park, NJ, August, 1999.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman andPatrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing: Multicast orBust*, Technical Report 99-1, Center for Information Technology Integration, January, 1999.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, Technical Report CSE-TR-376-98, Electrical Engineering and Computer Science, Universityof Michigan, , 1998.

Patrick McDaniel and Sugih Jamin, *A Scalable Key Distribution Hierarchy*, Technical Report CSE-TR-366-98, Electrical Engineering and Computer Science, Universityof Michigan, , 1998.

Patrick McDaniel and Peter Honeyman and Atul Prakash, *Lightweight Secure Group Communication*, Technical Report 98-2, Center for Information Technology Integration,University of Michigan, April, 1998.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0144

Wayne Zage and Delores Zage and Patrick McDaniel and IrshadKhan, *Evaluating Design Metrics on Large-Scale Software*, Technical Report SERC-TR-106-P, Software Engineering Resource Center, PurdueUniversity, September, 1991.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0145

# PUBLIC SPEAKING

*The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, University of California, Los Angeles, Los Angeles, CA, December, 2023.

*The Security of AI (what organizations need to know)*, TEDxUWMadison, Madison, WI, November, 2023.

*The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Michigan State University, Lansing, MI, November, 2023.

*The Security of AI (what organizations need to know)*, Greater Madison Chamber of Commerce, Madison, WI, September, 2023.

*Security's Role in Achieving Sustainability*, Center for Sustainability and the Global Environment, Madison, WI, February, 2023.

*Security's Role in Achieving Sustainability*, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.

*Security, Game Theory, and Their Role in Achieving Sustainability*, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.

*NSF Funding: Why, What and How*, School of Computer, Data & Information Sciences, UW-Madison, Madison, WI, October, 2022.

*Prognosticating the Future of IoT Security*, 2022 IEEE SafeThings Workshop, San Francisco, CA, May, 2022.

*The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Temple University, Philadelphia, PA, March, 2022.

*The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, CACR Security Speaker Series, Indiana University, Online, August, 2021.

*The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Robustness of AI Systems to Adversarial Attacks (RAISA3), Online, August, 2020.

*The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.

*The Challenges of Machine Learning in Adversarial Settings*, Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.

*The Challenges of Machine Learning in Adversarial Settings*, Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.

*The Challenges of Machine Learning in Adversarial Settings*, S2ERC, Ball State University, Muncie, IN, November, 2019.

*The Challenges of Machine Learning in Adversarial Settings*, Triangle Area Privacy and Security Day, Durham, NC, October, 2019.

*AI-Cybersecurity Workshop Briefing to the NITRD and MLAI Subcommittees*, NITRD and MLAI Subcommittees Quarterly Meeting, Washington, DC, July, 2019.

*Workshop on the Security and Privacy of Machine Learning*, Workshop on the Security and Privacy of Machine Learning, International Conference on Machine Learning, Long Beach, CA, June, 2019.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0146

*The Challenges of Machine Learning in Adversarial Settings*, 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.

*The Challenges of Machine Learning in Adversarial Settings*, National Science Foundation, Alexandria, VA, March, 2019.

*Convergence of AI and IoT*, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, The National Academy of Sciences/Engineering, Washington, DC, February, 2019.

*Tracing the Arc of Smartphone Application Security*, Duke University, Durham, NC, February, 2019.

*The Challenges of Machine Learning in Adversarial Settings*, Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.

*The Challenges of Machine Learning in Adversarial Settings*, Department of Computer Science, Purdue University, West Lafeyette, Indiana, November, 2018.

*The Challenges of Machine Learning in Adversarial Settings*, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, October, 2018.

*The Challenges of Machine Learning in Adversarial Settings*, Penn State University Alumni Association, University Park, PA, September, 2018.

*The Challenges of Machine Learning in Adversarial Settings*, Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

*Tracing the Arc of Smartphone Application Security*, School of Electrical and Computer Engineering, Georgia Tech University, Atlanta, GA, December, 2017.

*Tracing the Arc of Smartphone Application Security*, Department of Electrical Engineering and Computer Science, Ohio University, Athens, OH, October, 2017.

*Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings*, 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.

*Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings*, Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

*Tracing the Arc of Smartphone Application Security*, Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Collins, CO, October, 2017.

*Tracing the Arc of Smartphone Application Security*, Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

*Tracing the Arc of Smartphone Application Security*, University of Texas-Dallas, Department of Computer Science, Dallas, TX, May, 2017.

*Tracing the Arc of Smartphone Application Security*, 2017 ACM on International Workshop on Security And Privacy Analytics, Scottsdale, AZ, March, 2017.

*Tracing the Arc of Smartphone Application Security*, The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

*Tracing the Arc of Smartphone Application Security*, University of California-Irvine, Computer Science Department, Irvine, CA, March, 2017.

*Tracing the Arc of Smartphone Application Security*, Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

*Tracing the Arc of Smartphone Application Security*, 12th International Conference on Information Systems Security , Jaipur, India, December, 2016.

*Tracing the Arc of Smartphone Application Security*, University of Michigan, Ann Arbor, Ann Arbor, MI, November, 2016.

*Machine Intelligence in Adversarial Settings, Developing a Normative Framework for Cyberwarfare*, United States Naval Academy, Annapolis, MD, September, 2016.

*Eight Years of Mobile Smartphone Security*, University of Pittsburgh, Pittsburgh, PA, September, 2016.

*Eight Years of Mobile Smartphone Security*, New Jersey Institute of Technology, Newark, NJ, September, 2016.

*Setting a Cyber-Security Baseline for Physical Systems: Terminology, Technologies, and Goals*, Pacific Northwest Clean Water Association, webinar, August, 2016.

*The Limitations of Machine Learning in Adversarial Settings*, 25th International Conference on Computer Communication and Networks (ICCCN 2016), Waikoloa, HI, August, 2016.

*Learning from Ourselves: Where are we and where can we go in mobile systems security?*, Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.

*Eight Years of Mobile Smartphone Security*, Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.

*Eight Years of Mobile Smartphone Security*, University of Idaho, Moscow, ID, April, 2016.

*Army Installation 2035: Cyber Challenges and Opportunities*, US Department of Defense, Arlington, VA, April, 2016.

*The Limitations of Machine Learning in Adversarial Settings*, Florida Institute on National Security Assured Autonomy Workshop, Fort Myers, FL, February, 2016.

*SABOT: Specification-based Payload Generation for Programmable Logic Controllers*, Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) , San Francisco, CA, February, 2016.

*Seven Years of Mobile Smartphone Security*, Computer and Information Sciences Department, Temple University, Philadelphia, PA, January, 2016.

*Seven Years of Mobile Smartphone Security*, Massachusetts Institute of Technology–Lincoln Labs, Lexington, MA, January, 2016.

*Six Years of Mobile Smartphone Security*, Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, September, 2015.

*The Importance of Measurement and Decision Making to a Science of Security*, 2015 IEEE Conference on Communications and Network Security, Florence, Italy, September, 2015.

*The Importance of Measurement and Decision Making to a Science of Security*, 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.

*Six Years of Mobile Smartphone Security*, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrucken Germany, July, 2015.

*Six Years of Mobile Smartphone Security*, Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

*Estimating Attack Intent and Mission Impact From Detection Signals*, Workshop on Cyber Attack Detection, Forensics and Attribution forAssessment of Mission Impact, NATO Science and Technology Organization, Information Systems Technology Panel, Istanbul, Turkey, June, 2015.

*The Importance of Measurement and Decision Making to a Science of Security*, 2015 Symposium And Bootcamp on the Science of Security (Hotsos), University of Illinois at Urbana-Champaign, April, 2015.

*Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), Scottsdale, AZ, November, 2014.

*Evaluating Mobile Smartphone Security: The First Five Years*, Computer Science Colloquium Series, Harvard School of Engineering and Applied Sciences, Harvard University, Boston, MA, October, 2014.

*A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape*, IEEE New Technology Industry Seminar (NTIS '13), Everett, WA, August, 2013.

*Geotargeting: Mobile Device Privacy and Security*, National Academy of Sciences, Washington DC, February, 2013.

*Authentication and Web Security*, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, February, 2013.

*The Realities of Voting: A Retrospective of Ten Years of Information Security and Electronic Voting Systems*, 2012 Information Assurance Day, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, November, 2012.

*Permission-based Application Governance; A Step Forward or Backward?*, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July, 2012.

*Evaluating Mobile Smartphone Security: The First Four Years*, Carnegie Mellon University, Pittsburgh, PA, April, 2012.

*Scalable Integrity-Guaranteed AJAX*, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April, 2012.

*Evaluating Mobile Smartphone Application Security*, Singapore Management University, Singapore, September, 2011.

*Evaluating Mobile Smartphone Application Security*, Computer Security Foundations Symposium, Florham Park, NJ, July, 2011.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Computer Security Foundations Symposium, Domaine de l'Abbaye des Vaux de Cernay, France, June, 2011.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

*Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters*, Center for Non-Linear Studies, Los Alamos, NM, February, 2011.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Department of Software Information SystemsCollege of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, December, 2010.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Computer Science Department, Georgetown University, Washington D.C., November, 2010.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, University Park, PA, October, 2010.

*Security Challenges and Solutions in Mobile Smartphone Applications*, Security Day Seminar, Penn State University, University Park, PA, October, 2010.

*The Changing Vulnerability Landscape*, Association for Computing Machinery, Penn State Student Chapter, University Park, PA, September, 2010.

*The Changing Vulnerability Landscape*, ExxonMobil, Falls Church, VA, March, 2010.

*The Impact of Supply Chain on Information and Communications Technology Security*, The 1st Workshop on Telecommunications Infrastructure Protection and Security, Honolulu, HI, December, 2000.

*Energy Theft in the Advanced Metering Infrastructure*, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, State College, PA, October, 2009.

*Secure Provenance in High-End Computing Systems*, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2009.

*Missing Glue: Architectural Support for Security Annotations*, National Science Foundation Security Driven Architecture Workshop, Arlington, VA, July, 2009.

*Scalable Integrity-Justified Content Provenance*, NSERC ISSNet Workshop, Ottawa, Canada, June, 2009.

*Utility Grid Automation and Risk Management*, Clean Technology Conference and Expo, Houston, Texas, May, 2009.

*Scalable Integrity-Justified Content Provenance*, Center for Applied Cybersecurity Research, Indiana University, Bloomington, IN, April, 2009.

*Scalable Integrity-Justified Content Provenance*, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, April, 2009.

*What is Security*, Dickenson Law School, Penn State University, State College, PA, April, 2009.

*Scalable Integrity-Justified Content Provenance*, Department of Computer Science and Engineering, Notre Dame University, South Bend, IN, April, 2009.

*Electronic Voting: The Good, the Bad, and the Reality*, Software Engineering Research Center Showcase, Muncie, IN, November, 2008.

*Ohio Voting Systems Integrity: The EVEREST Report*, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, State College, PA, October, 2008.

*Data Provenance: Challenges and Technology*, Cyber Physical System Security Forum, Cyber SecurityResearch and Development Review, Washington DC, October, 2008.

*System-Wide Information Flow Enforcement*, NICIAR PI Meeting, Washington DC, September, 2008.

*Presto: Configuration Management at Massive Scale*, NSF Workshop on Assurable and Usable Security Configuration, George Mason University, Fairfax, VA, August, 2008.

*Asymmetry in Performance and Security Requirements for I/O in High-end Computing*, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2008.

*Authentication and Web Security*, Security and Privacy in IT-EMTM 604 Guest Lecture,University of Pennsylvania, Philadelphia, PA, May, 2008.

*SPAM and SPAM Mitigation*, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

*Phones, The Press, Research and Grad School ... or how to make trouble and have fun doing it*, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

*Applications and Services in Telecommunications Networks*, NSF Wireless Security Workshop, Georgia Institute of Technology, Atlanta, GA, March, 2008.

*Vulnerabilities and Opportunities in SMS-Capable Cellular Networks*, Computer Science Department, Carleton University, Ottawa, Canada, March, 2008.

*Ohio Voting Systems Integrity: The EVEREST Report*, Case-Western Reserve University, Cleveland, OH, February, 2007.

*Ohio Voting Systems Integrity: The EVEREST Report*, Ohio State University, Columbus, OH, February, 2007.

*Ohio Voting Systems Integrity: The EVEREST Report*, Ohio University, Athens, OH, February, 2007.

*Ohio Voting Systems Integrity: The EVEREST Report*, Miami University, Ohio, Oxford, OH, February, 2007.

*Ohio Voting Systems Integrity: The EVEREST Report*, Bowling Green State University, Bowling Green, OH, February, 2007.

*Vulnerabilities and Opportunities in SMS-Capable Cellular Networks*, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, September, 2007.

*Asymmetry in Performance and Security Requirements for I/O in High-End Computing*, HECIWG FSIO 2007 Workshop, NSF, Arlington, VA, August, 2007.

*Toward Valley-Free Interdomain Routing*, IEEE International Conference on Communications (ICC) 2007, Glasgow, Scotland, June, 2007.

*Extending Developer Tools for Security-Typed Languages*, Software Engineering Research Center FallShowcase, West Lafayette, IN, June, 2007.

*Open Functionality in SMS/Cellular Networks*, Computer and Information Science, University ofOregon, Eugene, OR, May, 2007.

*Open Functionality in SMS/Cellular Networks*, Computer Security Symposium, St. Cloud State University, St. Cloud, MN, May, 2007.

*Authentication and Web Security*, Security and Privacy in IT-EMTM 604 Guest Lecture,University of Pennsylvania, Philadelphia, PA, April, 2007.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0151

*Grains of SANs: Building Storage Area Networks from Memory Spots*, CISCO Remote Faculty Seminar, University Park, PA, April, 2007.

*Grains of SANs: Building Storage Area Networks from Memory Spots*, 2007 IEEE Security and Privacy Crystal Ball Workshop, Hawthorne, NY, January, 2007.

*Password Exhaustion: Predicting the End of Password Usefulness*, 2nd International Conference on Information Systems Security , Kolkata, India, December, 2006.

*Privacy Preserving Web-based Email*, 2nd International Conference on Information Systems Security, Kolkata, India, December, 2006.

*Physical and Digital Convergence: Where the Internet is the Enemy*, Eighth International Conference on Information andCommunications Security (ICICS '06), Raleigh, NC, December, 2006.

*Extending Developer Tools for Security-Typed Languages*, Software Engineering Research Center FallShowcase, Muncie, IN, November, 2006.

*Open Functionality in SMS/Cellular Networks*, Johns Hopkins University, Computer Science Department, Baltimore, MD, September, 2006.

*Open Functionality in SMS/Cellular Networks*, George Mason University, Computer Science Department, Fairfax, VA, September, 2006.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, Motorola Security Symposium, Itasca, Il, September, 2006.

*lseb: Testing Large Scale BGP Security in ReplayableNetwork Environments*, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

*BGPRV: A Library for Fast and Efficient Routing DataManipulation*, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

*JifClipse: Extending Developer Tools for Security-TypedLanguages*, Software Engineering Research Center SpringShowcase, Shaumburg, IL, June, 2006.

*Trends in Security: Critical Engineering in the Large*, Schlumberger InnovateIT! 2006, Cambridge, MA, May, 2006.

*Information Flow Revisited: Software Engineering toProvable Security*, Network Center of Excellence, Motorola Labs, Shaumburg, IL, May, 2006.

*Authentication and Web Security*, Security and Privacy in IT-EMTM 604 Guest Lecture,University of Pennsylvania, Philadelphia, PA, April, 2006.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, InfraGard Pittsburgh Chapter General Meeting, Pittsburgh, PA, March, 2006.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, Computer Science Department, University of Virginia, Charlottesville, VA, January, 2006.

*Software Engineering Tools for Security-Typed Languages:Using Eclipse to Make Secure Programming Practical*, Software Engineering Research Center Showcase, Muncie, IN, November, 2005.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, AT&T IP Services Security Council, Middletown, NJ, October, 2005.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0152

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, October, 2005.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, Computer Science Department, Yale University, New Haven, CT, October, 2005.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, October, 2005.

*Exploiting Open Functionality in SMS-Capable Cellular Networks*, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, State College, PA, October, 2005.

*lseb: Trace Driven Modeling of Internet-Scale BGP Attacksand Countermeasures*, 2nd Annual DETER/EMIST Workshop, Newport Beach, CA, September, 2005.

*Critical Infrastructure Security through Provably SecureNetwork Mediation*, 2nd Japan/US Workshop on Critical InformationInfrastructure Protection (CIIP), Tokyo, Japan, June, 2005.

*Extending Developer Tools for Security-typed Languages*, Software Engineering Research Center Showcase, West Lafayette, IN, June, 2005.

*Origin Authentication in Interdomain Routing*, 2005 IEEE Communications Quality and Reliability (CQR)International Workshop, St. Petersburg, FL, April, 2005.

*Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process*, Messiah College, Senior Seminar Series, Grantham, PA, April, 2005.

*Origin Authentication in Interdomain Routing*, Intel Research, Folsom CA, April, 2005.

*Key Distribution Strategies For Low-Power Wireless Networks*, Network Center of Excellence, Motorola Labs, Shaumburg, IL, April, 2005.

*Policy Evolution: Autonomic Environmental Security*, Software Engineering Research Center Showcase, Muncie, IN, December, 2004.

*Information Assurance for Enterprise Networks*, BAE Systems, Networking Seminar, Reston, VA, November, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science Department, Purdue University, West Lafayette, IN, October, 2004.

*Origin Authentication in Interdomain Routing*, Electrical Engineering and Computer ScienceDepartment, University of Michigan, Ann Arbor, MI, October, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science Department, University ofWisconsin, Madison, MD, September, 2004.

*Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process*, Computer Science and Engineering Student Organization, University Park, PA, September, 2004.

*Useless Metaphors? Why Specifying Policy is So Hard*, Workshop on Usable Privacy and Security Software,Center for Discrete Mathematics and Theoretical Computer Science(DIMACS), New Brunswick, New Jersey, July, 2004.

*Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process*, Information Systems Research Seminar, Stern School ofBusiness, New York University, New York, NY, April, 2004.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0153

*Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process*, Ball State University, Muncie, IN, April, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science Department, University of Illinois, Champaign, IL, March, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science and Engineering Department,University of Minnesota, Minneapolis, MN, March, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2004.

*Origin Authentication in Interdomain Routing*, Department of Computer Science, University ofMassachusetts - Amherst, Amherst, MA, March, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science and Engineering Department, PennState University, University Park, PA, March, 2004.

*Origin Authentication in Interdomain Routing*, School of Electrical Engineering and ComputerScience, Oregon State University, Corvallis, OR, February, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science Department, NorthwesternUniversity, Evanston, IL, February, 2004.

*Origin Authentication in Interdomain Routing*, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, February, 2004.

*Attack Profiling and Simulation in Interdomain Routing*, P2INGS Quarterly Meeting, Tempe, AZ, February, 2004.

*Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process*, AT&T Finance Lunch, Morristown, NJ, January, 2004.

*Origin Authentication in Interdomain Routing*, AT&T IP Security Conference, Middletown, NJ, November, 2003.

*Origin Authentication in Interdomain Routing*, 10th ACM Conference on Computer and CommunicationsSecurity (CCS), Washington, DC, October, 2003.

*Origin Authentication in Interdomain Routing*, Computer Science Department, Stevens Institute ofTechnology, Hoboken, NJ, October, 2003.

*Origin Authentication in Interdomain Routing*, Computer Science Department, Arizona State University, Mesa, AZ, September, 2003.

*Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process*, 31st Technology Policy Research Conference (TPRC), Arlington, VA, September, 2003.

*On Context in Authorization Policy*, 8th ACM Symposium on Access Control Models andTechnologies, Como, Italy, June, 2003.

*The Antigone Project*, DARPA Principal Investigator Meeting, San Antonio, TX, January, 2003.

*Methods and Limitations of Security Policy Reconciliation*, 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May, 2002.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0154

*Policy Management in Distributed Systems*, Cigital, Washington, DC, April, 2002.

*Antigone: Policy Management in Secure Group Communication*, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, April, 2001.

*Antigone: Policy Management in Secure Group Communication*, Computer Science Department, University of Wisconsin, Madison, MD, April, 2001.

*Antigone: Policy Management in Secure Group Communication*, Computer Science Department, University of Maryland, College Park, MD, April, 2001.

*Antigone: Policy Management in Secure Group Communication*, Computer Science Department, University of North Carolina, Chapel Hill, Chapel Hill, NC, April, 2001.

*Antigone: Policy Management in Secure Group Communication*, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2001.

*Antigone: Policy Management in Secure Group Communication*, AT&T Shannon Laboratory, Florham Park, NJ, February, 2001.

*Antigone: Policy Management in Secure Group Communication*, Telcordia Applied Research Laboratory, Morristown, NJ, February, 2001.

*Policy Problem Area 3 - Overview and Requirements*, Internet Engineering Task Force MSEC BOF, San Diego, CA, December, 2000.

*Multicast Security Policy Requirements and Building Blocks*, Quarterly Secure Multicast Research Group Meeting (SMuG), San Diego, CA, December, 2000.

*Antigone: Implementing Policy in Secure Multiparty Communication*, Systems Design and Implementation (SDI) / Laboratoryfor Computer Systems (LCS) seminar series, School of ComputerScience, Carnegie Mellon University, Pittsburgh, PA, November, 2000.

*Secure Group Communication in Antigone 2.0*, 11th Annual IPoCSE Research Symposium, Ann Arbor, MI, October, 2000.

*Antigone Secure Group Communication*, Bi-Annual DARPA Visit, Software System Research Laboratory, Ann Arbor, MI, September, 2000.

*Problem Area 3: Policy*, Quarterly Secure Multicast Research Group Meeting (SMuG), Pittsburgh, PA, July, 2000.

*Windowed Certificate Revocation*, IEEE INFOCOM 2000, Tel Aviv, Israel, March, 2000.

*A Response to 'Can We Eliminate Certificate Revocation Lists?'*, Financial Cryptography 2000, Anguilla, British West Indies, February, 2000.

*Multicast Security Policy Definition*, Quarterly Secure Multicast Research Group Meeting (SMuG), Washington, DC, November, 1999.

*Antigone: A Flexible Framework for Secure Group Communication*, Quarterly Secure Multicast Research Group Meeting (SMuG, NAI Labs, Baltimore, MD, September, 1999.

*Antigone: A Flexible Framework for Secure Group Communication*, 10th Annual IPoCSE Research Symposium, Ann Arbor, MI, September, 1999.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0155

*Antigone: A Flexible Framework for Secure Group Communication*, 8th USENIX Security Symposium, Washington, DC, August, 1999.

*Antigone: A Flexible Framework for Secure Group Communication*, IBM Watson Security Seminar, Westchester County, NY, July, 1999.

*Windowed Revocation in Public Key Infrastructures*, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1998.

*Scalable Key Distribution Hierarchy*, 9th Annual IPoCSE Research Symposium, Ann Arbor, MI, March, 1998.

*JavaLauncher Applet Platform*, NASA, Kennedy Space Center Security Seminar, Kennedy Space Center, FL, January, 1998.

*Secure High Performance Group Communication, Directed StudyDefense*, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1997.



EX-1003
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC
0156