

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAHOOT! ASA and KAHOOT EDU, Inc., Petitioner,
v.

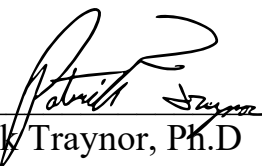
AVIEL D. RUBIN, Patent Owner.

Case IPR2023-00693
Patent 9,064,376 B1

DECLARATION OF PATRICK TRAYNOR, Ph.D.

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 further, 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 or Title 18 of the United State Code, and that such willful false statements may jeopardize the validity of the '376 Patent.

Date: November 30, 2023



Patrick Traynor, Ph.D

I. INTRODUCTION

1. My name is Patrick Traynor, Ph.D. I have been retained by Dr. Aviel D. Rubin which I may refer to as either the “Patent Owner” or “Dr. Rubin” for this *inter partes* review proceeding, which I may refer to as an “IPR.” I understand that this IPR proceeding involves U.S. Patent No. 9,064,376 (the “’376 Patent”). This declaration sets forth my opinions that the substitute claims set forth in Patent Owner’s Motion to Amend have support in the original disclosure of the application that led to the ’376 Patent. It is also my opinion that the substitute claims are valid over the prior art cited in the *inter partes* review.

2. I understand that Dr. Rubin is the inventor and owner of the ’376 Patent.

3. I understand that in this proceeding Kahoot! ASA and Kahoot EDU, Inc., which I may also refer to collectively as the “Petitioner” or “Kahoot,” filed a Petition for review of Claims 1-5, 9-10, 12-17 and 23-25 of the ’376 Patent.

4. I have reviewed and am familiar with the specifications, claims, and prosecution history of the ’376 Patent. Generally, I will cite to the ’376 Patent three ways. First, original Application 14/444,995 that gave rise to ’376 Patent is Patent Owner’s Exhibit 2005, and will be cited to as (Exhibit, Paragraph Number (s)). For example, the citation to paragraph seven of Application 14/444,995, will be Ex. 2005, ¶7. Second, provisional application No. 62/008,561, which is the

provisional application that the '376 Patent claims priority from, is Exhibit 2006, and will be cited to as (Exhibit, Paragraph Number (s)). Third, I will cite to the specification of the '376 Patent which is Petitioner's Exhibit 1001, using column and line numbers (Exhibit, Column: Line Number(s)). For example, the citation to the '376 Patent at column 1, lines 1 through 10, will be Ex. 1001, Col.1:1-10.

5. I understand that the Board has instituted the present IPR on the following grounds:

Claims Challenged	Basis	References
1-4, 9, 13-14, 16 and 23-25	Obviousness	Ground 1: <i>Zha</i> and a POSITA's "general knowledge"
1-4, 9, 13-14, 16 and 23-25	Obviousness	Ground 2: <i>Zha</i> , a POSITA's "general knowledge," and <i>Tsushima</i>
5, 15	Obviousness	Ground 3: <i>Zha</i> , a POSITA's "general knowledge," and <i>Gumbula</i>
5, 15	Obviousness	Ground 4: <i>Zha</i> , a POSITA's "general knowledge," <i>Tsushima</i> and <i>Gumbula</i>
10	Obviousness	Ground 5: <i>Zha</i> , a POSITA's "general knowledge," and <i>Stafford</i>
10	Obviousness	Ground 6: <i>Zha</i> , a POSITA's "general knowledge," <i>Tsushima</i> and <i>Stafford</i>
1-5, 9-10, 12-14, 16-17 and 23-25	Obviousness	Ground 7: <i>Takahashi</i> and a POSITA's "general knowledge"
1-5, 9-10, 12-14, 16-17 and 23-25	Obviousness	Ground 8: <i>Takahashi</i> and <i>Tsushima</i>

6. I have been asked to provide my objective, independent analysis of the '376 Patent, Patent Owner's proposed Substitute Claims provided in Patent Owner's Motion to Amend, and of the asserted prior art references cited in the

Petition, as well as to provide my opinion regarding the allegations in the Petition, as well as the supporting opinions of Dr. Sigurd Meldal.

7. I am not currently, nor have I ever been, an employee of Dr. Rubin. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the '376 Patent, the asserted prior art references cited herein and in the Petition, and any related issues. I will not receive any added compensation based on the outcome of this IPR, Patent Owner's Motion to Amend, any other IPR, or any other proceeding involving the '376 patent.

8. In forming my opinions expressed in this declaration, I have reviewed and, in some cases, relied upon the documents and other materials cited in Section III below, "Basis of Opinions and Materials Considered" in preparation of this declaration. To the best of my knowledge, those exhibits are true and accurate copies of what they purport to be. An expert in the field would reasonably rely on them to formulate opinions such as those set forth in this report.

9. This declaration contains opinions I formed with respect to the subject matter of this proceeding based on information available to date. I specifically reserve the right to formulate and offer additional opinions based on any additional information or discovery that may be provided or derived, and I likewise reserve the right to supplement my opinions based on future discovery or disclosures,

agreements between the parties, and additional evidence submitted by either party either prior to or at trial. I further reserve the right to supplement my opinions based on any expert testimony offered by Petitioner.

II. QUALIFICATIONS

10. My qualifications are listed in my Curriculum Vitae, which includes a complete list of my publications. Below, I summarize my qualifications and experience that qualify me to offer the opinions in this report as an expert.

11. I earned a B.S. in Computer Science from the University of Richmond in 2002 and an M.S. and Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2004 and 2008, respectively. My dissertation, entitled "Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks," focused on security problems that arise in cellular infrastructure when gateways to the broader Internet were created.

12. I am currently a Professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. I was hired under the "Rise to Preeminence" Hiring Campaign and serve as the Associate Chair for Research in my Department. I also hold the endowed position of the John and Mary Lou Dasburg Preeminent Chair in Engineering.

13. Prior to joining the University of Florida, I was an Associate Professor from March to August 2014 and an Assistant Professor of Computer Science from

2008 to March 2014 at the Georgia Institute of Technology. I have supervised many Ph.D., M.S., and undergraduate students during the course of my career.

14. My area of expertise is security, especially as it applies to mobile systems and networks, including cellular networks. As such, I regularly teach students taking my courses and participating in my research group to program and evaluate software and architectures for mobile and cellular systems. I have taught courses on the topics of network and systems security, cellular networks, and mobile systems at both Georgia Tech and the University of Florida. I also advised and instructed the Information Assurance Officer Training Program for the United States Army Signal Corps in the Spring of 2010.

15. I have received numerous awards for research and teaching, including being named a Kavli Fellow (2017), a Fellow of the Center for Financial Inclusion (2016), and a Research Fellow of the Alfred P. Sloan Foundation (2014). I also won the Lockheed Inspirational Young Faculty Award (2012), was awarded a National Science Foundation (NSF) CAREER Award (2010), and received the Center for Enhancement of Teaching and Learning at Georgia Tech's "Thanks for Being a Great Teacher" Award (2009, 2012, 2013).

16. I have published over 100 articles in top conferences and journals in the areas of information security, mobile systems, and networking. Many of my results are highly cited, and I have received multiple "Best Paper" Awards. I have

also written a book entitled "Security for Telecommunications Networks", which is used in wireless and cellular security courses at a number of top universities.

17. I am a Senior Member of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). I am also a member of the USENIX Advanced Computing Systems Association.

18. I serve as an Associate Editor for IEEE Security and Privacy Magazine, have been the Program Chair for eight conferences and workshops, and have served as a member of the Program Committee for over 50 different conferences and workshops. I am also currently the Security Subcommittee Chair for the ACM US Technology Policy Committee (USACM).

19. I was a co-Founder and Research Fellow for a private start-up, Pindrop Security, from 2012 to 2014. Pindrop provides anti-fraud and authentication solutions for Caller-ID spoofing attacks in enterprise call centers by creating and matching acoustic fingerprints. Pindrop Security currently employs over 200 people, and their technology is based off of my research (US Patent 9,037,113 B2).

20. I was a co-Founder and Chief Executive of a private start-up, CryptoDrop. CryptoDrop developed a ransomware detection and recovery tool to provide state of the art protection to home, small business, and enterprise users. This technology was also based off of my research (US Patent 10,685,114 B2).

21. I was also a co-Founder and Chief Executive of a private start-up, Skim Reaper. Skim Reaper developed tools to detect credit card skimming devices, and worked with a range of banks, international law enforcement, regulators, and retailers. This technology was also based off of my research (US Patent 10,496,914 B2).

22. I am a named inventor on ten US patents. These patents detail methods for determining the origin and path taken by phone calls as they traverse various networks, cryptographically authenticating phone calls, providing a secure means of indoor localization using mobile/wireless devices, detecting credit card skimmers, identifying cloned credit cards, and blocking ransomware from encrypting data. My curriculum vitae, attached as Appendix A, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

23. I am very familiar with and have substantial expertise in the area of information security, mobile systems, and networking.

III. MATERIALS CONSIDERED

24. I have reviewed the '376 Patent, including the challenged claims, and its prosecution history. I have also reviewed the Petition for inter partes review filed by Petitioner, as well as the Exhibits attached, including:

- 25. Ex. 1004: U.S. Patent No. 9,497,565 (“*Zha*”)
- 26. Ex. 1005: CN 2013/10674692 (“*Zha* Priority Application”)
- 27. Ex. 1006: Certified English translation of the *Zha* Priority Application
- 28. Ex. 1007: U.S. Patent Pub. No. 2015/0011318 (“*Takahashi*”)
- 29. Ex. 1008: PCT/JP2012/007595 (“*Takahashi Priority Application*”)
- 30. Ex. 1009: Certified English translation of *Takahashi Priority*

Application

- 31. Ex. 1010: U.S. Patent Pub. No. 2014/0006485 (“*Tsushima*”)
- 32. Ex. 1011: U.S. Patent No. 9,591,083 (“*Gumbula*”)
- 33. Ex. 1012: U.S. Patent Pub. No. 2012/0017236 (“*Stafford*”)
- 34. Ex. 1013: U.S. Patent No. 9,330,531 (“*Wakeford*”)
- 35. Ex. 1014: Patent Owner’s Preliminary Infringement Contentions in *Rubin v. Kahoot! ASA et al.*, Civil Action No. 6:22-cv-00236 (W.D. Tex.) (Sept. 28, 2022)

- 36. Ex. 1015: U.S. Patent Pub. No. 2012/0253841 (“’841 Application”)
- 37. Ex. 1016: U.S. Patent Pub. No. 2012/0209770 (“’770 Application”)
- 38. Ex. 1017: U.S. Patent Pub. No. 2014/0121015 (“*Massing*”)
- 39. Ex. 1018: U.S. Patent Pub. No. 2006/0058088 (“*Crawford*”)
- 40. I have also reviewed various other sources cited within this declaration.

41. In forming my opinions, I have considered the materials listed above and any documents cited in this declaration. I have also relied on my own education, knowledge, and experience in the relevant art.

34. I have also considered the understanding of a POSITA around the time of the invention the '376 Patent.

IV. LEGAL PRINCIPLES

35. I am not an attorney and will not offer opinions on the law.

36. In forming the analyses and conclusions expressed in my declaration, I have applied the legal principles described in the following paragraphs, which were provided to me by counsel for the Patent Owner.

A. Priority

37. I understand that a patent may claim the benefit of the filing day of an earlier filed application if the earlier filed application provides adequate disclosure of the patent's claims. I understand that the disclosure requirement is satisfied if a POSITA could clearly conclude that the inventor invented the claimed subject matter as of the earlier filing date sought. I understand that the earlier filed application does not need to describe the claimed subject matter in precisely the same terms as found in the claims at issue.

B. Obviousness

38. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been

obvious to a person of ordinary skill in the art at the time of the alleged invention (“POSITA”), taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include “long felt need” for the claimed invention, commercial success attributable to the claimed invention, unexpected results of the claimed invention, skepticism of others, failure by others to achieve the claimed invention, and “copying” of the claimed invention by others.

39. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason that would have prompted a POSITA to modify the single prior art reference, or combine two or more references, in a manner that provides the elements of the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference(s) themselves, the knowledge or “common sense” of a POSITA, or from the nature of the problem to be solved, and this reason may be explicit or implicit from the prior art as a whole. I have been informed that, under the law, the combination of familiar elements according to known methods is likely to be obvious when it does no more than

yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

C. Analogous Art

40. I understand that a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). *See* MPEP § 2141.01(A). I understand that “‘same field of endeavor’ and ‘reasonably pertinent’ are two separate tests for establishing analogous art; it is not necessary for a reference to fulfill both tests in order to qualify as analogous art.” MPEP § 2141.01(A).

41. When determining whether the “relevant field of endeavor” test is met, the one should consider “explanations of the invention’s subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.” *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380 (Fed. Cir. 2019); MPEP § 2141.01(A). “When determining whether a prior art reference meets the ‘same field of endeavor’ test for the analogous art, the primary focus is on what the reference discloses.” *Airbus S.A.S.*, 941 F.3d at 1380; MPEP § 2141.01(A).

42. To determine if a reference is “reasonably pertinent,” one should “consider the problem faced by the inventor, as reflected - either explicitly or

implicitly - in the specification. In order for a reference to be 'reasonably pertinent' to the problem, it must 'logically [] have commended itself to an inventor's attention in considering his problem.'" *In re ICON Health and Fitness, Inc.*, 496 F.3d 1374, 1379-80 (Fed. Cir. 2007); MPEP § 2141.01(A). "An inventor is not expected to have been aware of all prior art outside of the field of endeavor." *Airbus*, 41 F.3d at 1380-82; MPEP § 2141.01(A). "A reference outside of the field of endeavor is reasonably pertinent if a person of ordinary skill would have consulted it and applied its teachings when faced with the problem that the inventor was trying to solve." *Airbus*, 41 F.3d at 1380-82; MPEP § 2141.01(A).

D. Claim Construction

34. I understand that claim construction is a matter that will be decided by the Board presiding over this IPR. I understand that the relevant inquiry in claim construction is the question of how a POSITA would have understood the claim terms at the time of the earliest priority date, in light of the patent specification, the prosecution history, and any other relevant intrinsic and extrinsic evidence.

V. PERSON OF ORDINARY SKILL IN THE ART

35. All of the opinions that I express here have been made from the standpoint of a person of ordinary skill in the art at the time of the invention of the '376 Patent, which I may refer to as a "POSITA."

36. I understand that, for the purposes of this proceeding, the '376 patent is entitled to a priority date of no later than July 28, 2014.

37. I understand that the Petitioner has proposed that a POSITA at about the priority date of the '376 patent would have had “a bachelor’s degree in electrical or computer engineering or computer science or a comparable field of study, plus approximately two years of professional experience in the field of computer and/or network design and security or other relevant industry experience.” Ex. 1002, ¶31.

38. I understand that in the Institution Decision the Board adopted Petitioner’s statement of the level of ordinary skill in the art. I further understand the Patent Owner did not file a substantive response to the Petition, and therefore Board was not presented with an alternative hypothetical level of ordinary skill.

39. For the purposes of this proceeding, I mostly agree with Petitioner’s proposed level of skill with some clarification and adjustment. In my opinion, a POSITA at the relevant time frame would have a bachelor’s degree in electrical or computer engineering or computer science or a comparable field of study, plus approximately two years of professional experience in the field of computer and security and/or network design and security. Petitioner’s proposed catchall statement “or other relevant industry experience” is vague and unhelpful.

40. At the relevant time frame, I was a person of more than ordinary skill in the art during the relevant timeframe. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

VI. CLAIM CONSTRUCTION

41. I understand that in the Institution Decision the Board declined to expressly construe any claim terms. I further understand that the Board did not analyze any other claims besides Claim 1. I generally construed all the terms of the '376 Patent consistent with how a POSITA would understand the plain and ordinary meaning of the terms as of the '376 Patent priority date. However, I believe the term “sensitive information” in original claim 3, and Substitute Claims 28, 30, 35, 37 and 38 requires claim construction in light of arguments made by Petitioner which I address in paragraphs 101-105 below.

42. Substitute Claim 28, which replaces original claim 3, claims: “The method of claim 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information.” The '376 Patent provides a number of examples of “sensitive information” including a poker player’s “hole cards” (Ex. 2005, ¶¶21-23), a bank account balance (Ex. 2005, ¶57), and healthcare records (Ex. 2005, ¶78). The '376 Patent specification teaches that when practicing the claims '376 Patent, sensitive

information should not be shared with the first device because the first device may be compromised by malware. Ex. 2005, ¶¶ 20, 23, 55, 63-65, 78. An exception to this requirement is where connection is lost with the second device, and the user gives permission to the application before sensitive information is shared with the first device. Ex. 2005, ¶¶34-35. Based on the language of the claims, and the teachings of the '376 Patent, it is clear that a POSITA would understand “sensitive information” sent to second device at a minimum is information that the application will not automatically share with the first device without first seeking the user’s permission.

VII. WRITTEN DESCRIPTION

43. I have reviewed the proposed Substitute Claims 26-41 attached to Patent Owner’s Motion to Amend. Using the limitations of the Substitute Claims, I have prepared a table showing each limitation of the Substitute Claims as well as the paragraphs (and/or page numbers) to the excerpts from Dr. Rubin’s original Provisional Application No. 62/008,561 and/or the Patent Application No. 14/444,995 supporting the Substitute Claims:

Claim	Claim Element of Substitute Claim	'561 P.App	'995 App.
[26Pre]	A method for transmitting information to multiple electronic devices, the method comprising:	[TBD]	¶2; ¶18-19; ¶23-25;
[26a]	electronically storing a set of information at a server;	[TBD]	Fig. 5; Fig. 6; ¶25; ¶38; ¶39; ¶89-90;

Decl. ISO Patent Owner's Mot. to Amend
Case No. IPR2023-00376

[26b]	identifying a first subset of the information and identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	[TBD]	¶23-28; ¶38
[26c]	determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.	[TBD]	Fig. 10; ¶26; ¶33; ¶75; ¶83; ¶89; ¶90; ¶92
[26d]	if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device.	[TBD]	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; ¶23-29 ¶33-34; ¶58; ¶65; ¶78; ¶82
[27]	The method of claim <u>26</u> , further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.	[TBD]	¶24; ¶38-39; ¶45; ¶48

[28]	The method of claim <u>26</u> , wherein	[TBD]	
[28a]	the first subset of the information comprises non-sensitive information; and	[TBD]	¶30-32
[28b]	the second subset of the information comprises sensitive information.	[TBD]	¶30-32; ¶35; ¶57; ¶78; ¶82
[29]	The method of claim <u>26</u> , wherein the information received at the second device is more sensitive than the information received at the first device.	[TBD]	¶24; ¶30-32; ¶35; ¶57; ¶78;
[30]	The method of claim <u>28</u> , further comprising: determining if connectivity between the server and the second device has been disrupted; and providing a notification by the application on the second device that the connectivity has been disrupted.	[TBD]	¶33; Claim 5 (p.28)
[31]	The method of claim <u>26</u> , wherein the transmitting a first subset of the information to the first device from the server and transmitting a second subset of the information to the second device from the server are executed over independent electronic communications networks.	[TBD]	Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35;
[32]	The method of claim <u>26</u> , further comprising displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.	[TBD]	¶45; ¶48;
[33]	The method of claim <u>26</u> , wherein the information received at the second device is a user's private cards in an online card game.	[TBD]	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48
[34]	The method of claim <u>26</u> , wherein the a display on the first device is being	[TBD]	Fig. 2; Fig. 4; Fig. 5; Fig. 6;

Decl. ISO Patent Owner's Mot. to Amend
Case No. IPR2023-00376

	viewed exclusively by a first user and a display on a second device is also being viewed exclusively by the first user.		¶25-26; ¶31; ¶35; ¶39; ¶45; ¶48; ¶57; ¶65; ¶78
[35]	The method of claim <u>30</u> , wherein, neither the first subset of information nor the second subset comprise a two factor authentication code, and, further comprising displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.	[TBD]	¶45; ¶48
[36]	The method of claim <u>26</u> , wherein the server is a proxy server configured to relay communications from an application server to the first and second devices wherein the proxy server emulates a client to the application server.	[TBD]	¶50; ¶52
[37]	The method of claim <u>26</u> , further comprising configuring the server for managing an online game, and wherein the server is configured to communicate with a plurality of devices including a first electronic device and a second electronic device, wherein the first electronic device is primarily used to play the game, and wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.	[TBD]	¶23; ¶25; Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35; Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48
[38]	The method of claim <u>37</u> , wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.	[TBD]	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48
[39]	The method of claim <u>26</u> , further comprising electronically storing at the	[TBD]	¶25-26; ¶31; ¶33-34; ¶35

	server a parameter indicating whether subsets of the information are to be divided between two or more devices.		
[40]	The method of claim 26, wherein the first and second subsets of information are application-specific, and wherein the first and second subsets of information derive from functions within a specific application.	[TBD]	¶20-23; ¶55 ¶57; ¶77-78
[41pre]	A system for transmitting information to multiple electronic devices, the system comprising:	[TBD]	¶2; ¶18-19; ¶23-25
[41a]	an electronic data store configured for electronically storing a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	[TBD]	Fig. 5; Fig. 6; ¶25; ¶38; ¶39; ¶89-90
[41b]	a processor device programmed for:	[TBD]	¶81; ¶98 ¶¶101-102
[41c]	identifying a first subset of the information and identifying a second subset of the information;	[TBD]	¶23-28; ¶38
[41d]	determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information at both the first and second devices wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device;	[TBD]	Fig. 10; ¶26; ¶33; ¶75; ¶83; ¶89; ¶90; ¶92

[41e]	if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device.	[TBD]	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; ¶23-29 ¶33-34; ¶58; 65; ¶78; ¶82
-------	--	-------	---

VIII. THE PROPOSED SUBSTITUTE CLAIMS COMPARED TO THE INSTITUTED GROUNDS AND ART

44. I am informed that a Patent Owner does not bear the burden of proving the patentability of substitute claims. I am informed that Petitioner has the burden of prove unpatentability by a preponderance of the evidence.

45. I have reviewed Patent Owner's proposed Substitute Claims. For my analysis below, I have focused on the primary references, *Takahashi* and *Zha*, and secondary reference, *Tsushima*, relied upon in the Petition.

46. The Substitute Claims distinguish the cited references relied upon in the Board's institution decision with respect to independent claims 1 and 25 (corresponding to Substitute Claims 26 and 41). It is my opinion that the proposed Substitute Claims are patentable over the cited art.

47. Also, amendments the Patent Owner made to dependent claims 5 and 14 (corresponding to Substitute Claims 30 and 35) establish further additional basis to

distinguish the cited references relied upon by the Petitioner with respect to these claims.

A. *Zha*

48. I have reviewed the proposed substitute claims in comparison with *Zha*. Ex. 1004. It is my opinion that the proposed substitute claims are patentable over *Zha*.

49. *Zha* discloses a method for “displaying an interfaces, an apparatus, a terminal and a server.” Ex. 1004, Col.1:17-18. The “problem” identified by *Zha* is use of an application program with more than one “functional interface,” such as a “microblog”¹ with a “homepage interface,” a “private messaging interface” and a “game interface.” Ex. 1004, Col.1:23-27. If the user is using the homepage functional interface on their terminal, but wants to send a private message to a friend (what people typically refer today as sending a “direct message” or “DM”), the user must operate their terminal to exit the homepage functional interface and then enter the private message functional interface. Ex. 1004, Col.1:28-32. *Zha* explains that “[s]ince the application program may provide multiple functional interfaces” the user must operate their terminal to “switch” between the various

¹ Well known microblogs that existed at the time *Zha* was published included Twitter, Facebook, Instagram, Tumblr, Reddit and LinkedIn. Ex. 2007 (<https://www.linkedin.com/pulse/guide-through-7-microblogging-websites-realytvviews/>).

functional interfaces the user desires to access. Ex. 1004, Col.1:33-36. This “switching process” requires the terminal to download “related data from the server, thereby increasing a network traffic imperceptibly.” Ex. 1004, Col.1:37-39. Further, *Zha* states that when switching frequently amongst functional interfaces, the “user needs to operate the terminal to switch between different functional interfaces back and forth, thus an operational complexity for the user is high.” Ex. 1004, Col.1:39-43.

50. *Zha* discloses a “method for displaying an interface . . . where the first terminal and a second terminal currently use an application program with one account.” Ex. 1004, Col.2:1-5. *Zha* disclose using “access permissions for different functional interfaces . . . assigned to terminals which simultaneously use an application program with one account.” Ex. 1004, Col.2:59-63. *Zha* further discloses that “data corresponding to each of the functional interfaces is only assigned to a terminal having an access permission for the functional interface, instead of assigning the data corresponding to each of the functional interfaces to all the terminals using the application program.” Ex. 1004, Col.2:62-67.

51. According to *Zha*, this separation of data “solv[es] the problem that the consumption of network traffic is large in conventional technology and reducing the network traffic occupied in assigning the data corresponding to different functional interfaces to the terminals.” Ex. 1004, Col.2:67-3:4. *Zha* adds that

“operational complexity for the user” is reduced by having multiple terminals receive only the data for their assigned functional interface and thus reducing the need for “frequent switching operations.” Ex. 1004, Col.3:3-14.

52. Substitute Claim 26 and 41 (formerly claim 1 and 25) have added the requirement of “*using application specific authentication information* at both the first and second devices, *wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.*” Appendix A (Listing of Claims), pp. 3, 8. *Zha* does not mention or disclose the use of authentication information to determine if a first user is logged into the application. More specifically, *Zha* does not mention or disclose the use of authentication information that is “application specific” and that the application specific authentication information is different for determining login to the application at the first and second devices.

53. *Zha* discloses generally that the “user may login to a microblog in the laptop computer, the cellphone and the desktop computer with one microblog account.” Ex. 1004, Col.6:56-61. This generic discussion is repeated throughout *Zha*:

For example, microblog may provide a homepage functional interface, a private message functional interface and a game functional interface. The server, on receiving that the cellphone logs in to microblog with

the same account, may assign an access permission for accessing the homepage interface to a laptop computer which has logged in to microblog and assign an access permission for accessing the private message interface to a cellphone which logs in to microblog. Similarly, when a desktop computer logs in to microblog with the same account, the server may assign an access permission for accessing the game interface to the desktop computer.

Ex. 1004, Col.7:33-4; *see also* Col.8:60-67, Col.9:18-38, Col.12:46-56, Col.14:4:12, Col.17:44-54, Col.18:11-20, 39-46.

54. It is my opinion that a POSITA would understand the disclosure of *Zha*, which discusses generically “logging in” on two different terminals with the “same account” does not disclose the specific authentication requirements called for by Substitute Claim 26 and 41 (and their dependents). *Zha* does not teach or disclose using application specific authentication information to log into the application on the first and second device, or that the application specific authentication information must be different between the first device and second device.

1. *Zha* Is Not Analogous Prior Art.

55. Petitioner’s reliance on *Zha* is misplaced because, in my opinion, a POSITA would not consider *Zha* analogous prior art. As noted above, I have been informed an asserted reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention or (2) the

reference is reasonably pertinent to the problem faced by the inventor. *Zha* is neither.

56. The field of endeavor for the '376 Patent is online security. Notably, that is Dr. Rubin's personal background as professor emeritus at Johns Hopkins University in the field of computer security. See Johns Hopkins University website at <https://engineering.jhu.edu/faculty/aviel-rubin/>. More specifically, the '376 Patent plainly states that the field of invention relates to "securing communications against malware by utilizing two devices with differential or application-specific component during an online session." Ex. 2005, ¶2. This is supported by the claims which claim use of applications designed to use two device, and only when the user is authenticated on both devices, transmit select data to only one of the two devices in case malware has compromised the other device. See, e.g., Ex. 2005, pp. 27-28 (original proposed Claims 1 and 3).

57. *Zha*, on the other hand, is directed towards "interface display" on multiple terminals. Nothing in *Zha* relates to the field of online security generally, or securing communications against malware more specifically. While *Zha* in its broadest sense, relates to an interface display method for multiple devices using the same application, it is much narrower in application because *Zha*'s method is only applicable to online applications with more than one functional interface. For the

vast majority of online applications that offer a single functional interface, *Zha* has no application.

58. *Zha* attempts to solve a much different problem than '376 Patent. As discussed above, *Zha* assigns different access permissions for applications with more than one functional interface so that each terminal only receives data specific to its assigned functional interface. According to *Zha*, this helps to reduce (i) network traffic and (ii) switching by the user. The '376 Patent seeks to improve on the prior art of "two-factor authentication" by disclosing a system and method where "the user has persistent use of a first device and a second device throughout the use of an online application to prevent a compromise of the transaction if malware infects either device." Ex. 2005, ¶18. The two problems being solved for are completely unrelated.

59. Because *Zha* pertains to a different "field of endeavor" than the '376 Patent, and attempts to solve a different problem than the '376 Patent, in my opinion *Zha* is not analogous prior art.

2. Motivation to Combine.

60. Another issue with *Zha* is that a POSITA would not have looked to *Zha* by itself, or in combination with other references or the general knowledge of a POSITA, to achieve the claims of the '376 Patent. As discussed above, *Zha* is far afield. I agree with the Petitioner, in part, that a relevant POSITA would have

background and/or training in computer security, but *Zha* has nothing to do with security. Indeed, the words security or secure are never used in *Zha*, and the concept of security is never discussed.

61. *Zha* is also limited to online applications with different functional interfaces. As noted in every claim of *Zha*, an application program must have a “functional interface to the first terminal being distinct at least in part from the assigned functional interface assigned to the second terminal.” *See, e.g.*, Ex. 1004, Col. 29:31-33. This makes sense for *Zha* because unless an application program has more than one functional interface to choose from, there is no reason to apply the teachings of *Zha* in order to reduce the network traffic or lower the amount of switching between functional interfaces to decrease “operational complexities.” A POSITA would not look far afield to *Zha* which is directed to a very small subset of applications in order to achieve the claims of the '376 Patent which have a much broader application in the field of online security.

3. *Zha* Does Not Disclose “Sensitive Information”

62. Substitute Claims 28, 30, 35, 37 and 38 all incorporate the limitations from original Claim 3 that “the First subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information.” Ex. 2005, pp. 27. Substitute Claim 28, 30, 35, 37 and 38 all depend from Substitute Claim 26 that specifies “the first and second subsets of information

are generated by the same application at the server and are specific to that application.” Ex. 2005, pp. 27 (emphasis added).

63. Petition argues that *Zha*’s “private message interface data” corresponds to the “sensitive information” limitation in original claim 3. Ex. 1002, ¶¶99-100 (“*Zha* discloses the server sends the private message to the cellphone terminal, which corresponds to the claimed ‘transmitting a second subset of the information to the second device from the server.’”). There are several reasons why this argument is wrong. The “sensitive information” that is sent to the second device must be (per Substitute Claim 26), “sensitive information” that was (i) *generated by the application* (ii) *at the server* and (iii) *specific to the application*. Petitioner points to “private messages” sent via the private message interface, but this alleged sensitive information (i.e., private messages) is generated by the users (not the “same application”), on the user’s device (not the server), and private messages are not specific to any application. The users could send and/or exchange their private messages on any messaging application.

64. Finally, as discussed more below with respect to the *Takahashi* reference, I do not believe the term “sensitive information” properly construed would include messages on *Zha*’s private message interface without additional teaching in *Zha*. As discussed below, “sensitive information” claimed in Substitute Claims 28, 30, 35, 37 and 38, is directed to information that the application will not

share with the first device out of concern the first device is compromised by malware. There is no disclosure or teaching in *Zha* that the messages a user would typically send on one of the multiple direct messaging applications (like Facebook or Instagram direct messaging) would be of the same sensitive nature as the “sensitive information” claimed in the '376 Patent that should not be viewed/received on the user's other devices running the same application. Petitioner cannot twist *Zha*'s private messaging interface into a disclosure of transmitting the claimed sensitive information (that would not be shared with the first device because of concerns of malware) “generated by the application” “at the server” and “specific to the application.”

B. *Tsushima*

65. Petitioner argues that *Zha* in combination *Tsushima* (Grounds 2, 4 and 8) discloses all the limitations of, and renders obvious, claims 1-5, 9-10, 13-16 and 23-25. Petitioner relies on *Tsushima* for the disclosure of original claim 1 “if and only if limitation.” Ex. 1002, ¶155. I do not address Petitioner's argument that *Tsushima* discloses the “if and only if limitation” because it is not relevant to my overall opinion as to why the proposed amendments overcome Petitioner's cited prior art. However, *Tsushima* contains some discussion regarding “logging in” to a first device and second device which Petition may argue discloses aspects of the proposed amendments in Substitute Claims 26 and 41. *See, e.g.*, Ex. 1010, ¶¶57-61.

None of Tsushima's discussion of "logging in" discloses the added limitations to Substitute Claims 26, 41 and their dependent claims.

66. *Tsushima* discloses a "content providing system and control method" using a server, a first device which is a "portable terminal" used for "operational input," and a second device which is the "display device" and may be a number of devices including a "game console, a set top box, a portable game device, a PDA, a tablet or the like." Ex. 1010, ¶28. Figure 5 of *Tsushima* discloses game processing for a game system that involves the logging in of the first and second devices. Ex. 1010, Fig. 5. *Tsushima* discloses a process where in step 501 the portable terminal/first device "***receives input of account information from the user***, and determines whether or not login to a service provided by the server 200 succeeded." Ex. 1010, ¶57. In step 502, the second device "***receives account information input from the user*** and determines whether or not login to a service that the server 200 provides succeeded." Ex. 1010, ¶58.

67. *Tsushima* next discloses step S503 where the "server CPU" determines:

[W]hether or not login to a service succeeded on both an operation input device (the portable terminal 100) and a screen display device (the PC 300) for ***a user ID that is a target of service provision***. Specifically, when there is a request to login to a service, ***the server CPU 201 checks the validity of account information included in the login request***. Next, in a case where the validity of a login request was confirmed, the server CPU 201 associates the user ID that is logging in, and

identification information of the device being used to log in, and stores this in the server RAM 203

Ex. 1010, ¶59 (emphasis added).

68. In step S503 where the server CPU “determines that login has succeeded for both an operational input device and a screen display device for a provision target user ID,” it moves the processing to step S504. Ex. 1010, ¶61. The foregoing represents the totality of *Tsushima*’s discussion of “logging in” at both devices.

69. The foregoing shows that *Tsushima* does not disclose being logged into the application using “authentication information” and/or “application specific authentication information.” *Tsushima* only discloses receiving “account information input” which *Tsushima* states “may be managed with, for example, a password 702 associated with a user ID 701 as shown in FIG. 7A.” Ex. 1010, ¶41. *Tsushima* says nothing about whether any authentication information is “application specific,” and instead uses more generic language that “account information of users of *a service that the server 200 provides* is managed in the server ROM 202.” Ex. 1010, ¶41 (emphasis added). Further, *Tsushima* does not teach or disclose that the application specific authentication information used to login to the first device is different than the application specific authentication information used to login to the second device.

70. It is my opinion that a POSITA would understand *Tsushima* does not disclose use of application specific authentication information at both the first and second device where the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.

1. *Tsushima* Is Not Analogous Prior Art.

71. It is my opinion a POSITA would not consider *Tsushima* analogous prior art.

72. As discussed above, the field of endeavor for the '376 Patent is plainly online security. The '376 Patent states that the field of invention relates to “securing communications against malware by utilizing two devices with differential or application-specific component during an online session.” Ex. 2005, ¶2. This is supported by the claims which claim use of applications designed to use two device, and only when the user is authenticated on both devices, transmit select data to only one of the two devices in case malware has compromised the other device. *See, e.g.*, Ex. 2005, pp.27-28 (original proposed Claims 1 and 3).

73. *Tsushima*, on the other hand, is directed towards “a content providing system, a control method thereof, and particularly to a streaming distribution technique for encoded video data.” Ex. 1010, ¶2. Additionally, *Tsushima* states “The

present invention relates to a content providing system and a control method, and particularly to a technique of loading static data into shared memory.” *Id.*

74. *Tsushima* field of endeavor and description of related art has no relation to computer security. *Tsushima*’s “Summary of Invention” describes inventing a “content providing system, and a control method thereof, that realizes a content service in which it is possible to provide a wide range of operation input to a user.” Ex. 1010, ¶11. *Tsushima*’s “Summary of Invention” further describes two aspects of the present invention including the use of a first device for operational input, a server for receiving the operational input, updating the display based on the operational input, and transmitting the updated display to a second “display unit.” Ex. 1010, ¶¶ 12, 13.

75. Consistent with the above description of the Summary of Invention, *Tsushima* claims a “content providing system” and “control method for a content providing system” comprising a first device for operational input, a server for receiving and updating screen and transmitting to a second device for display. *See, e.g.,* Ex. 1010, Claim 1 and 8.

76. Similar to *Zha*, *Tsushima* field of endeavor has nothing to do with computer security. *Tsushima* is focused on improving upon the conventional techniques of experiencing streaming video data whether from network games or a

“video distribution service.” Nothing in *Tsushima* relates to the field of online security generally, or securing communications against malware more specifically.

77. *Tsushima* is also directed to a much different problem than '376 Patent. As discussed above, the '376 Patent is directed at responding to malware that may have compromised a user's device. The '376 Patent addresses this problem by using online applications designed to require two devices where chosen information is only disclosed to the second device in case the first device is compromised by malware. Ex. 2005, ¶¶3-7. *Tsushima*, on the other hand, seeks to provide a wider range of “operational inputs” for a user when using a mobile device as the controller for a video display (whether a game or a video) on a separate “display device.” Ex. 1010, ¶¶10-11. There is simply no relation to the problem addressed by *Tsushima* and the problem addressed by the '376 Patent.

78. Because *Tsushima* pertains to a different “field of endeavor” than the '376 Patent and attempts to solve a different problem than the '376 Patent, in my opinion *Tsushima* is not analogous prior art.

2. Motivation to Combine *Tsushima* with *Zha*.

79. Another issue with *Tsushima* is that a POSITA would not have looked to combine *Tsushima* with *Zha*. As discussed above, *Tsushima* is equally far afield from the '376 Patent as *Zha*. A POSITA would have background and training in

computer security, but *Tsushima* has nothing to do with security and is outside the POSITA's relevant field.

80. Unlike the '376 Patent that is device agnostic – meaning any two capable electronic devices can be used to practice the claims – *Tsushima* is device specific. Ex. 2005, ¶19 (“Any combination of electronic devices can be used.”). *Tsushima* teaches that its first device is a “portable terminal.” Ex. 1010, ¶28 (“For example, the portable terminal 100 may be a device, such as a portable game device, a mobile phone, a PDA, a tablet or the like.”). *Tsushima* further teaches the second device is a “PC” that may include a game console, a set top box, a portable game device, a PDA, a tablet or the like.” Ex. 1010, ¶ 28.

81. As discussed above, *Zha* and *Tsushima* seek to address completely different problem. *Zha* seeks to limit the display of different functional interfaces of applications (such as a microblog) to specific terminals of a user so as (i) to reduce network traffic and (ii) the switching between functional interfaces within the application. *Tsushima* seeks to provide a wider range of operational inputs for a control device that were limited under the prior art techniques.

82. *Zha* also has a very narrow focus on online applications with more than one functional interface that can be bifurcated onto multiple terminals. Conversely, *Tsushima* is limited to games services or video services split onto two devices that

performs the processing of the “service” at the server instead of the client devices.

Ex. 1010, ¶¶9-11, pp. 5-6 (claims 1 and 8).

83. Even if the combination of *Zha* and *Tsushima* disclosed all the limitations of Substitute Claims 1-5, 9-10, 13-16 and 23-25, which in my opinion they do not, a POSITA would not have been motivated-to-combine the two references to achieve the claims of the '376 Patent. Both references are far outside the field of computer security, and both seek to address different problems from each other, and from the problems addressed in the '376 Patent. Further, *Zha*'s purpose is very narrowly focused on addressing the small number of applications (such as microblogs like Twitter and Facebook) with more than one functional interface, where *Tsushima* is a device specific display mechanism for graphic intensive services where processing of the video is done at a server instead of the user's end-device. The claims of the '376 Patent require use of an application that is designed for use by two devices, where *Zha* targets a specific type of application with multiple functional interfaces (*i.e.*, microblogs) that does not require the use of two devices. *Zha* improves the use of these specific applications by employing more than one device, but these applications do not require two devices unlike all the claims of the '376 Patent. *Tsushima* is even more narrowly focused on video “services” processed at the server and employing specific types of devices for the “portable terminal” and “display device.”

84. The motivation-to-combine *Zha* and *Tsushima* becomes even more attenuated with respect to the dependent Substitute Claims. In particular, Substitute Claims 28, 30, 35, 37 and 38 (original claims 3, 5, 10, 16, 17) all require transmission of (i) “non-sensitive information” to the first device that is (ii) generated by the application (iii) at the server, and (iv) is specific to that application, and transmission of (i) “sensitive information” to the second device that is (ii) generated by the application (iii) at the server, and (iv) is specific to that application. These Substitute Claims solve the problem of malware potentially compromising the first device by directing the “sensitive information” to the second device. *Zha* and *Tsushima* are so far afield of computer security and seek to address such totally unrelated problems, a POSITA would not be motivated to combine their teachings to arrive at these Substitute Claims.

85. In summary, it is my opinion that *Tsushima* does not disclose the new limitations Substitute Claims 26 and 41 (Original Claims 1 and 25). Specifically, *Tsushima* does not disclose *using application specific authentication information at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.* Moreover, for reasons discussed above, *Tsushima* is not analogous prior art to the '376 Patent, nor would a POSITA have been motivated to combine *Tsushima* with *Zha*.

C. Takahashi

86. I have reviewed the proposed substitute claims in comparison with *Takahashi*. Ex. 1007. It is my opinion that the proposed substitute claims are patentable over *Takahashi*.

87. *Takahashi* field of invention relates to “a technique for controlling game progress with a communications terminal of a user via a communications network.” Ex. 1007, ¶2. *Takahashi* states that the object of the invention is directed to a “game control device, a non-transitory computer readable recording medium, a game control method, and a game control system that allows a variety of types or forms of games by use of a plurality of communications terminals.” Ex. 1007, ¶6.

88. The “problem” identified by *Takahashi* is that a user of a social network games uses a “mobile communication terminal irrespective of where the user is.” Ex. 1007, ¶5. In light of this, *Takahashi* states “it is difficult to realize a variety of types or forms of games on the assumption that the user uses a single communication terminal.” Ex. 1007, ¶5.

89. Unlike the '376 Patent, which is directed at applications that require the use of two devices to secure an online transaction, *Takahashi* game control device and system applies equally to one device, or multiple devices. Ex. 1007, Fig. 9, ¶81, 86.

90. Substitute Claims 26 and 41 (formerly original claim 1 and 25) add the requirement of determining at the server whether the first and second device are in possession of and being directly operated by a first user “based on the first user being logged into the application *using application specific authentication information* at both the first and second devices, *wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.*” Appendix A (Listing of Claims), pp. 3, 8. *Takahashi* does not disclose logging in using application specific authentication information that is different for the first and second devices.

91. First, *Takahashi* discloses a login process which is then followed separately by an authentication process. For example, Figure 11 of *Takahashi* discloses a process where a registered user “logs in to the game server.” Ex. 1007, ¶110, Fig. 11 (showing “Authentication processing” “after user logs in.”). *Takahashi* does not disclose anything further regarding the login process. Accordingly, on its face, *Takahashi* does not disclose being logged into the application using application specific authentication information at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.

92. Only after the user “logins to the game” does *Takahashi* disclose an authentication process, that uses “identification information, or the user ID and the password” to authenticate the user. Ex. 1007, ¶110. *Takahashi*’s “mobile terminal 10” makes an HTTP access request to the game server that includes “identification information.” Ex. 1007, ¶110. *Takahashi*’s second device, PC12, transmits an HTTP access request using “user ID and a password that have been inputted to the PC12.” Ex. 1007, ¶110. The “game server 20” then performs “authentication processing (Step S12).” Ex. 1007, ¶110.

93. *Takahashi* teaches that “identification information” used by the mobile device for user authentication is “unique information for each mobile terminal.” Ex. 1007, ¶74. In particular, *Takahashi* states “identification information” may be “a serial number of the mobile terminal” or a “user agent character string in a HTTP request” from the mobile terminal to the game server. Ex. 1007, ¶74. A POSITA would understand, consistent with *Takahashi*’s teaching, that this “identification information” is authentication information that is specific to the device. Meaning it is authentication information that is not “application specific,” but device specific.

94. Every disclosed embodiment of *Takahashi* includes at least the use of one mobile device (*see, e.g.*, Ex. 1007, Fig. 1, 7-9,15, 18, 20), which means every authentication process in *Takahashi* involves the use of device specific authentication information. In no circumstance does *Takahashi* disclose using

“application specific” only authentication information for both devices that is also different for the first device and second device. For example, in *Takahashi* where the first and second device are both mobile devices, the authentication information may be different (i.e., different serial numbers), but the authentication information is device specific, not application specific. Where the first and second devices are both “PCs” (an embodiment *Takahashi* does not disclose), the authentication information is a “user ID and password” which may be application specific authentication information but it is the same for both devices. Finally, where the first device is a mobile terminal and the second device is a PC, the authentication information between the two devices may be different, but the mobile terminal uses device specific authentication information instead of application specific authentication information.

95. In sum, *Takahashi* discloses an entirely different login and authentication process than Substitute Claims 26 and 41. Substitute Claims 26 and 41 require a user to be logged in via an authentication process using application specific authentication information at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device. *Takahashi* clearly discloses an authentication process that occurs after a user has logged into *Takahashi*'s game server. Moreover, in all the various possible

combinations of authentication using two devices, *Takahashi* fails to disclose using application specific authentication information at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device. If anything, *Takahashi* teaches away from using “application specific authentication information” that is different for the first and second device by requiring that the mobile devices in *Takahashi* use “identification information” that is device specific.

1. *Takahashi Is Not Analogous Prior Art*

96. In my opinion a POSITA would not consider *Takahashi* analogous prior art. As discussed above, the field of endeavor for the '376 Patent is online security. While the preferred embodiment is directed to “online games” the invention can be applied to any number of online activities “such as online banking, mobile healthcare, online investing, and other online activities that would benefit from enhanced security against malware on a user's computing device.” Ex 2005, ¶20. Accordingly, a POSITA would not look broadly to “online games”, “online banking”, “mobile healthcare”, “online investing” and “other online activities” for prior art relevant to the '376 Patent, unless the prior art was also directed to enhancing security. Otherwise, the scope of potentially relevant prior art would be unbounded.

97. *Takahashi* is directed to “a game control device” for online games.

Takahashi's field of endeavor relates to techniques “for controlling game progress with a communications terminal.” Ex. 1007, ¶2. Nothing in *Takahashi* relates to the field of online security generally, or securing communications against malware more specifically. Additionally, Dr. Rubin's invention is directed at securing online transactions within an application designed specifically to utilize two external devices. *Takahashi*'s “game control device” works with one device, or two devices. So even in the vast field of online games, *Takahashi* “game control device” is directed at online games using at least one external device, where all the online applications that could apply the teachings of the '376 Patent require two devices.

98. *Takahashi* attempts to solve a much different problem than '376 Patent. As discussed above, *Takahashi* is directed to a “game control device” that can be carried out on one device, or two devices. The '376 Patent attempts to secure online transactions by use of two devices. Because *Takahashi* attempts to solve a different problem, and is in a different field of endeavor from the '376 Patent, it is my opinion *Takahashi* should not be considered analogous prior art.

2. Motivation to Combine *Takahashi*

99. Another issue with *Takahashi* is that a POSITA would not have looked to *Takahashi* by itself, or in combination with other references, to achieve the claims of the '376 Patent. As discussed above, *Takahashi* is far afield. A POSITA

would have background and training in computer security, but *Takahashi* has nothing to do with securing online transactions, gaming or otherwise.

100. Additionally, the '376 Patent is directed solely at applications designed to employ two devices to secure the desired online transaction. *Takahashi* is not so limited. *Takahashi*'s "technique for controlling game progress with a communication terminal" works with one device, or two devices. As such, as POSITA would not look to *Takahashi* to achieve the claims of the '376 Patent because the '376 Patent is limited to applications using two devices.

3. *Takahashi* Does Not Disclose "Sensitive Information"

101. Substitute Claims 28, 30 and 35 all incorporate the limitations from original Claim 3 that "the First subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information." Substitute Claim 28, 30 and 35 all depend from Substitute Claim 26 that specifies "the first and second subsets of information ***are generated by the same application at the server and are specific to that application.***" *Id.* (emphasis added).

102. Petition argues that *Takahashi* discloses sending only "sensitive information" to the second device based on *Takahashi*'s disclosure of sending "user-specific information" to the *Takahashi*'s mobile device. Ex. 1002, ¶261. Petitioner argues that the user's "game results" could be "sensitive" information because

“knowing another player’s score could provide a player with an unfair advantage.”

Ex. 1002, ¶262.

103. I respectfully disagree that *Takahashi*’s “game results” constitute the disclosure of “sensitive information” claimed in the Substitute Claims. *Takahashi*’s “game results” cannot be “sensitive information” claimed in Substitute Claims and sent only to the second device because *Takahashi* teaches sharing the same “sensitive information” with the first device. In Figure 9, and related disclosure in paragraph 86, *Takahashi* teaches playing the fishing device on a single mobile device where the “game contents of two images illustrated in FIG. 8 may be displayed on the mobile terminal 10. . . . In the example of FIG. 9, a display region 150 is provided on the display screen of the mobile terminal 10 to indicate catches in fishing.” Ex. 1002, ¶86. The ’376 Patent discloses that “sensitive information” is at a minimum, information that the application will not share with the first device out of concern the first device is comprised by malware. *Takahashi*’s “game results” are shared with the user’s first device if/when the user plays their fishing game on a single device.

104. Additionally, *Takahashi* teaches sharing “game results” amongst the users in multi-player embodiments, which is predictable and common practice for the social network type games described in *Takahashi*. Ex. 1007, ¶¶129, 135, 142.

Accordingly, *Takahashi*'s "game results" cannot be "sensitive information" as claimed in Substitute Claims.

105. The above further demonstrates why *Takahashi*'s one device, or two device, configuration teaches away from motivating a POSITA to combine the teachings of *Takahashi* to achieve the claims of the '376 Patent. *Takahashi* does not take into consideration the sensitivity of the information sent to the two different devices, as the moment the user switches to a single device (or begins play with a single device) all of the separated information that maybe "sensitive information" is exposed to a single device that is potentially compromised by malware. This is opposite to the security objectives of the '376 Patent.

4. *Takahashi* Does Not Disclose "providing a notification by the application on the second device that the connectivity has been disrupted."

106. It is proposed to amend Claim 5 (Substitute Claim 30), by adding "providing a notification by the application on the second device that the connectivity has been disrupted."

107. Petitioner argues that *Takahashi* discloses "providing a notification on the second device that the connectivity has been disrupted" because if a user is playing the fishing game using a web browser the web browser will detect if the connection has been disrupted and notify the user. Ex. 1002, ¶265. Dr. Rubin's proposed amendment to Substitute Claim 30 makes clear that the application

responsible for generating the first and second subsets of information which are specific to that application is also the same application responsible for providing notification on the second device that the connectivity has been disrupted.

108. Petitioner relies on the web browser providing the user notification on the first device, which is not the same application in *Takahashi* that generates the first and second subsets of information and transmits that information to the first and second devices. In *Takahashi*, it is the fishing game that generates the first and second subsets of information and transmits that information to the first and second devices. Accordingly, *Takahashi* does not disclose “providing a notification by the application on the second device that the connectivity has been disrupted.”

IX. CONCLUSION

109. I currently hold the opinions that I have expressed in this declaration. However, my analysis may continue, and I may acquire or receive additional information or insights that may result in revised or supplemental observations or opinions.

Patrick Gerard Traynor

Professor

Associate Chair for Research in CISE

John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)

University of Florida

E301 CSE Building, PO Box 116120

Gainesville, FL 32611 USA

traynor@cise.ufl.edu

<http://www.cise.ufl.edu/~traynor>

Table of Contents

EDUCATIONAL BACKGROUND	4
EMPLOYMENT HISTORY	4
CURRENT FIELDS OF INTEREST	4
I. TEACHING	6
A. Courses Taught	6
B. Continuing Education	6
C. Curriculum Development	6
D. Individual Student Guidance	7
E. Teaching Honors and Awards	11
II. RESEARCH AND CREATIVE SCHOLARSHIP	12
A. Thesis	12
B. Published Journal Papers (Refereed)	12
C. Published Books and Parts of Books	13
D. Edited Proceedings	14
E. Conference Presentations	14
E.1. Conference Presentations with Proceedings (Refereed)	14
E.2. Conference Presentations with Proceedings (Non-Refereed)	19
E.3. Conference Presentations without Proceedings	19
F. Other	19
F.1. Submitted Journal Papers	19
F.2. Refereed Research Reports	20
F.3. Software	20
F.4. Published Papers (Non-Refereed)	20
F.5. Books in Preparation	20
F.6. Workshops and External Courses	20
G. Research Proposals and Grants (Principal Investigator)	21
H. Research Proposals and Grants (Contributor)	23
I. Research Honors and Awards	24
III. SERVICE	25
A. Professional Activities	25
A.1. Memberships and Activities in Professional Societies	25
A.2. Conference Committee Activities	25
B. On-Campus Committees	26
B.1. University of Florida	26
B.2. Georgia Tech	27
C. Special Assignments	27
D. Ph.D. Examining Committees	27
E. External Member of M.S. Examining Committee	31
F. Consulting and Advisory Appointments	31
G. Civic Activities	31
IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION	32
A. Honors and Awards	32
B. Invited Conference Session Chairmanships	32
C. Professional Registration	32
D. Patents	32
E. Editorial and Reviewer Work for Technical Journals and Publishers	33
F. Expert Witness Services	35
V. OTHER CONTRIBUTIONS	36
A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)	36

B. Special Activities 39

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2008	Pennsylvania State University State College, PA <i>Dissertation:</i> Characterizing the Impact of Ridigity on the Security of Cellular Telecommunications Networks <i>Advisors:</i> Thomas F. La Porta and Patrick D. McDaniel	Computer Science & Engineering
M.S.	2004	Pennsylvania State University State College, PA	Computer Science & Engineering
B.S.	2002	University of Richmond Richmond, VA <i>Minors:</i> Biology, Business Admin	Computer Science

EMPLOYMENT HISTORY

Title	Organization	Years
Professor	University of Florida	August 2018–Present
Associate Professor	University of Florida	August 2014–July 2018
Associate Professor	Georgia Institute of Technology	March 2014–August 2014
Assistant Professor	Georgia Institute of Technology	2008–March 2014
Research Assistant	Pennsylvania State University	2004–2008
Teaching Assistant	Pennsylvania State University	2004

CURRENT FIELDS OF INTEREST

My research focuses on the security of cellular/telephony networks and mobile systems. The security of these systems generally relies on their closed nature and trust in the honest behavior of users. However, with the recent disintegration of these assumptions and with over than six billion subscribers around the world, cellular and mobile systems represent the next great expansion in global critical infrastructure and, because of their unique characteristics, require new and different approaches to security.

Recognizing this, my research focuses on three specific themes: (1) developing efficient techniques to allow telephony providers and customers to authenticate the origin of incoming calls; (2) measuring and improving the security of emerging mobile financial systems and (3) efficient and strong privacy-preserving techniques for mobile devices. Additionally, I have significant expertise in fraud detection, particularly for payment systems.

I have a strong interest in solutions that can be deployed in both the short and long terms, and am actively engaging both industry and government in this capacity. My research, if successful, will help to not only improve the general security of networked devices, but also to maintain the historical reliability of telephony networks as they become the dominant digital access technology.

I. TEACHING

A. Courses Taught

Semester/Year	Course Number & Title	Number of Students	Comments
Fall 2021	CNT 5410 Computer and Network Security	45	New Topics
Fall 2019	CNT 5410 Computer and Network Security	28	New Topics
Fall 2018	CIS 6930 Cellular and Mobile Network Security	16	New Course
Fall 2017	CNT 5410 Computer and Network Security	27	New Topics
Fall 2016	CNT 5410 Computer and Network Security	60	New Topics
Spring 2016	CNT 5410 Computer and Network Security	13	New Topics
Spring 2015	CNT 5410 Computer and Network Security	12	New Topics
Fall 2014	CNT 5410 Computer and Network Security	30	New Course
Spring 2014	CS 6262 Network Security	55	New Projects
Fall 2013	CS 3251 Computer Networks I	73	Expanded Syllabus
Spring 2013	CS 6262 Network Security	65	All New Projects
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2012	CS 8803 Cellular & Mobile Network Security	17	New Topics
	CS 8001 Information Security Seminar	20	New Speakers
Spring 2011	CS 8001 Information Security Seminar	20	New Speakers
Fall 2011	CS 6262 Network Security	27	Expanded Syllabus
	CS 8001 Information Security Seminar	35	New Speakers
Spring 2011	CS 3251 Computer Networks I	61	Expanded Syllabus
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2010	CS 8803/4803 Cellular & Mobile Network Security	16	New Course
	CS 8001 Information Security Seminar	31	New Speakers
Fall 2009	CS 6262 Network Security	55	Expanded Syllabus
Spring 2009	CS 3251 Computer Networks I	45	Expanded Syllabus
Fall 2008	CS 8003 Destructive Research	10	New Course

Guest lecturer for CS 4235 (Introduction to Information Security) and CS 8803 (e-Democracy) in Fall 2008.

Advised ECE 4811/CS 4802 (Vertically Integrated Project) with Ed Coyle

B. Continuing Education

None.

C. Curriculum Development

CS 8803 Cellular and Mobile Network Security: *Fall 2010.* Developed an entirely new course around security issues facing cellular and mobile networks. Students learned about wireless basics, spectrum issues, core network architectures (GSM, ISDN, IMS, SIP), air interfaces (GSM, 3G), mobility management, authentication, mobile phone operating systems (Android, iPhone), Android security, congestion and denial of service, privacy and eavesdropping. Students also complete a research project and aim towards publishing this work at a major venue. My aim is for this class to become part of the regular offering of security courses and receive a non-8803 number. Semester projects were also judged and encouraged using a “venture capital” model, in which students had to pretend as if they were pitching their ideas for a start-up company to potential investors.

CS 6262 Network Security: *Fall 2009.* Totally rewrote the syllabus and slide material, giving the class its first major overhaul in a number of years. While many old themes remain, new lecture blocks including Web Security, Cellular Security and Social Engineering were developed from scratch. This new course material was made available to all other faculty members teaching this class, who have since used my slides and syllabus.

CS 3251 Computer Networks I: *Spring 2009.* Modified undergraduate networking course to include a persistent focus on security at all layers of the protocol stack. I have also created new lectures focusing on the physical layer and cellular networks and new exams to include all of the abovementioned changes.

CS 8803 Destructive Research: *Fall 2008.* Developed course based around understanding how so-called secure systems have been defeated by attackers. With such knowledge, students would have the context to develop the next generation of more secure systems. I delivered more than 1/3 of the lectures in this seminar course and paid special focus on vulnerabilities in cellular networks, analog telecommunications and electronic voting. Students were also instructed on techniques for performing research, writing technical papers and making conference and lecture-style presentations. I have offered these slides to future 7001 classes to help impact a wider audience.

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2009–Fall 2013

Her research discovered vulnerabilities in mobile web browsers and developed techniques to detect malicious mobile web pages. Joined Oracle in Spring 2014.

Jasmine Bowers University of Florida

Fall 2015–Summer 2020

Her research focuses on mobile applications, and the development of tools for building secure systems. Now: Research Scientist, MITRE

Henry “Hank” Carter Georgia Institute of Technology

Fall 2010–Spring 2016

Developing techniques for secure function evaluation for privacy-preserving applications on constrained mobile devices. Now: Assistant Professor, Villanova University

Italo Dacosta Georgia Institute of Technology

Fall 2008–Summer 2012

Co-advised with Mustaque Ahamad. Research on scaling performance of SIP network components. Graduated Summer 2012, currently research scientist at EPFL.

David Dewey Georgia Institute of Technology

Fall 2011–Summer 2015

Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.

Brad Reaves University of Florida
Fall 2014–Spring 2017
Develop strong authentication techniques for cellular networks. Now: Assistant Professor at North Carolina State University.

Nolen Scaife University of Florida
Fall 2014–Spring 2019
Developed techniques to detect credit card skimming. Now: Assistant Professor at the University of Colorado Boulder

2. Ph.D. Students Supervised

Hadi Abdullah University of Florida
Fall 2016–Present
Evaluating the security of ML-driven voice interfaces.

Logan Blue University of Florida
Fall 2016–Present
Investigating facial feature reconstruction from voice recordings.

Cassidy Gibson University of Florida
Fall 2019–Present
Investigating weaknesses in web software.

Daniel Olszewski University of Florida
Fall 2019–Present
Removing unwanted/insecure features from software.

Christian Peeters University of Florida
Fall 2016–Present
Develop techniques to detect and defend against call and message interception attacks in cellular networks.

Imani Sherman University of Florida
Fall 2018–Present
Developing usable interfaces against robocalls. Co-advised with Juan Gilbert.

Luis Vargas University of Florida
Fall 2016–Present
Developing techniques for network-based detection and mitigation of malware in a healthcare environment.

Kevin Warren University of Florida
Fall 2019–Present
Detecting deepfake audio through linguistic information.

3. Ph.D. Students - Other

Saurabh Chakradeo Georgia Institute of Technology
Fall 2010–Spring 2013
Research exploring malicious mobile applications. Left to join Facebook.

Brendan Dolan-Gavitt Georgia Institute of Technology
Spring 2009
Research project on using kernel type graphs to detect dummy structures.

Eric (Yu) Liu Georgia Institute of Technology

Fall 2008

Research on the spread of malware through cellular infrastructure.

Chaz Lever Georgia Institute of Technology

Fall 2011–Spring 2014

Developing techniques to measure the spread of malware in cellular networks. Left Georgia Tech to create a startup.

Frank Park Georgia Institute of Technology

Fall 2008–Spring 2010

Research on multi-factor authentication using cellular phones. Left program after failing comprehensive exam to join startup.

Ferdinand Schober Georgia Institute of Technology

Fall 2009–Summer 2010

Developed mechanisms for smart networks and smart mobile devices to fight infection and provide remote remediation. Returned to Microsoft.

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2008–Spring 2009

Research on improving performance of security critical functions in IMS cellular core. Completed her Ph.D with me at GT.

Logan Blue University of Florida

Fall 2015–Spring 2016

Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology

Fall 2009–Spring 2010

Research on security issues caused by transitive trust assumptions in the Windows COM infrastructure. Completed his Ph.D. with me at GT.

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

Developed continuous authentication mechanisms using the multitude of sensors available on a mobile phone. Now at Bishop Fox Consulting (industry).

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

Performed research that compared the security vulnerabilities found in the traditional and mobile web.

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

Research on building a real-time streaming audio system using attribute-based crypto for broadcast encryption.

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

Discovered hijacking attacks in SNMPv3, a widely used and thought to be secure network management protocol. Now at Solute (industry).

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

Research on developing an iPhone application to prevent individuals from being profiled by Shopper Loyalty Programs. First with MIT Lincoln Labs, now with Trail of Bits.

Rishikesh Naik Georgia Institute of Technology

Fall 2008–Spring 2010

Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal CISE

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

Research on creating provably anonymous networks on a base of secure function evaluation. Now with VMWare.

Walter “Nolen” Sciafe Georgia Institute of Technology

Spring 2012–Spring 2014

Developed the OnionDNS architecture, which prevents domain delisting attacks by leveraging a Tor hidden service. Joined Ph.D. program at UF.

Tyler Tucker University of Florida

Fall 2018–Present

Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology

Spring 2009

Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology

Spring 2013

Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology

Spring 2011

Developed mobile phone-based tools for measuring performance and reachability throughout the Internet.

Ashwin Narasimhan Georgia Institute of Technology

Spring 2009

Research on developing efficient security mechanisms for the IMS cellular core.

Aamir Poonawalla Georgia Institute of Technology

Spring 2010

Helped develop a call provenance infrastructure, which included both networking and machine learning components.

Erin Reddick Georgia Institute of Technology

Fall 2008–Fall 2009

Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology

Spring 2009

Research on developing efficient security mechanisms for the IMS cellular core.

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology

Spring 2014

Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology

Fall 2011–Spring 2012

Developed a mobile phone application for taking measurements of cellular networks.

Dane Van Dyck Georgia Institute of Technology

Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

1. Georgia Institute of Technology, CETL “Thanks For Being A Great Teacher” Award, Fall 2013.
2. Georgia Institute of Technology, CETL “Thanks For Being A Great Teacher” Award, Fall 2012.
3. United State Army Signal Corps, “Helmet” Award, 2010.
4. Georgia Institute of Technology, CETL “Thanks For Being A Great Teacher” Award, Spring 2009.
5. Pennsylvania State University CSE Graduate Student Teaching Award, 2005

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

1. Patrick Gerard Traynor. *Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks*. PhD thesis, The Pennsylvania State University, May 2008.

B. Published Journal Papers (Refereed)

1. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1), 2018.
2. Patrick Traynor, Kevin Butler, Jasmine Bowers, and Bradley Reaves. FinTechSec: Addressing the Security Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.
3. Nolen Scaife, Henry Carter, Rachel Jones, Lyrissa Lidsky, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. *International Journal of Information Security (IJIS)*, 2017.
4. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bharatiya, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Security (TOPS)*, 2017.
5. Henry Carter and Patrick Traynor. OPFE: Outsourcing Computation for Private Function Evaluation. *International Journal of Information and Computer Security (IJICS)*, 2017.
6. Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, William Enck, Negar Kiyavash, Ahmad-Reza Sadeghi, and Patrick Traynor. Phonion: Practical Protection of Metadata in Telephony Networks. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017.
7. Bradley Reaves, Jasmine Bowers, Sigmond A. Gorski III, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. *droid: Assessment and Evaluation of Android Application Analysis Tools. *ACM Computing Surveys (CSUR)*, 2016.
8. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor. Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing (TMC)*, To Appear 2016.
9. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. *Journal of Security and Communication Networks (SCN)*, To Appear 2016.
10. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. *Journal of Computer Security (JCS)*, 24(2):137–180, 2016.
11. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security (JCS)*, 23(2):167–195, 2015.
12. Henry Carter, Chaitrali Amrutkar, Italo Dacosta, and Patrick Traynor. For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices. *Journal of Security and Communication Networks (SCN)*, 7(7):1165–1176, 2014.
13. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. *IEEE Transactions on Mobile Computing (TMC)*, 14(5), 2015.

14. Andrew Harris, Seymour Goodman, and Patrick Traynor. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 2013.
15. Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1), 2012.
16. Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa Ammar, and Ellen Zegura. ARDEN: Anonymous netwoRking in Delay tolERant Networks. *Journal of Ad Hoc Networks*, 10(6):918–930, 2012.
17. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.
18. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 22(11):1804–1812, 2011.
19. Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. From Mobile Phones to Responsible Devices. *Journal of Security and Communication Networks (SCN)*, 4(6):719 – 726, 2011.
20. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. *Journal of Computer Security (JCS)*, 18(5):799–837, 2010.
21. Patrick Traynor, Kevin Butler, William Enck, 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, 2010.
22. Patrick Traynor. Securing Cellular Infrastructure: Challenges and Opportunities. *IEEE Security & Privacy Magazine*, 7(4), 2009.
23. Kevin Butler, Sunam Ryu, 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, 2009.
24. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks On Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, 17(1), 2009.
25. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TISSEC)*, 2008.
26. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.
27. Patrick Traynor, Raju Kumar, Heesook Choi, Sencun Zhu, Guohong Cao, and Thomas La Porta. Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. *IEEE Transactions on Mobile Computing (TMC)*, 6(6), 2007.

C. Published Books and Parts of Books

1. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. *Emerging Privacy and Security Concerns for Digital Wallet Deployment*. Privacy in America: Interdisciplinary Perspectives. Scarecrow Press, July 2011.

2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. *Privacy Preserving Web-Based Email*. Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.
3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Presentations with Proceedings (Refereed)

1. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022.
2. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Communications Information and Internet Policy (TPRC 49)*, 2021.
3. Hadi Abdullah, Kevin Warren, Vincent Bindschaedler, Nicolas Papernot, and Patrick Traynor. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021.
4. Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, Logan Blue, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, and Patrick Traynor. Hear “No Evil”, See “Kenansville”: Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021.
5. Imani Sherman, Jasmine Bowers, Liz-Laure Laborde, Juan E. Gilbert, Jaime Ruiz, and Patrick Traynor. Truly Visual Caller ID? An Analysis of Anti-Robocall Applications and their Accessibility to Visually Impaired Users. In *IEEE International Symposium on Technology and Society (IEEE ISTAS)*, 2020.
6. Imani Sherman, Jasmine Bowers, Keith McNamara, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2020. (Acceptance rate: 17.4%).
7. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 17.0% for full papers).
8. Vanessa Frost, Dave Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. Examining DES-based Cipher Suite Support within the TLS Ecosystem. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 22.0% for all papers).
9. Dave Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. A Practical Intel SGX Setting for Linux Containers in the Cloud. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY’19)*, 2019. (Acceptance rate: 23.5%).

10. Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani Sherman, Lisa Anthony, and Patrick Traynor. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. (Acceptance rate: 12.0%).
11. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019. (Acceptance rate: 25.6%).
12. Hadi Abdullah, Washington Garcia, Christian Peeters, P. Traynor, K. Butler, and J. Wilson. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
13. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
14. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.
15. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
16. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. Attention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
17. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).
18. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
19. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
20. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).
21. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).
22. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).

23. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
24. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
25. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).
26. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).
27. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).
28. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).
29. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).
30. Nolen Scaife, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).
31. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
32. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
33. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).
34. Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).
35. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).
36. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).

37. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).
38. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).
39. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).
40. Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2012. (Acceptance rate: 25%) (Best Paper - SAIC Student Paper Competition (GT)) (Finalist - CSAW AT&T Applied Security Research Best Paper Competition 2012).
41. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. A Measurement Study of SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? In *Proceedings of the Information Security Conference (ISC)*, 2012. (Acceptance rate: 32%) (Best Student Paper).
42. Italo Dacosta, Mustaque Ahamad, and Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012. (Acceptance Rate: 20.2%).
43. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2012. (Acceptance Rate: 17.8%).
44. Yacin Nadji, Jon Giffin, and Patrick Traynor. Automated Remote Repair for Mobile Malware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
45. Nilesh Nipane, Italo Dacosta, and Patrick Traynor. "Mix-In-Place" Anonymous Networking Using Secure Function Evaluation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
46. Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011. (Acceptance Rate: 13.9%).
47. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding Individual User Profiling in Shopper Loyalty Programs. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, 2011. (Acceptance Rate: 35.1%).
48. David Dewey and Patrick Traynor. No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2011. (Acceptance Rate: 20.1%).
49. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDrOp: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).

50. Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. In *IEEE Global Communications Conference (GLOBECOM)*, 2010. (Acceptance Rate: 35.6%).
51. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2010. (Acceptance Rate: 25.0%).
52. Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating Bluetooth as a Medium for Botnet Command and Control. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2010. (Acceptance Rate: 30.7%).
53. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).
54. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).
55. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
56. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
57. Italo Dacosta, Vijay Balasubramanian, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).
58. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).
59. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).
60. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).
61. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).
62. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).
63. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).

64. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).
65. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).
66. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).
67. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).
68. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).
69. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).
70. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

E.2. Conference Presentations with Proceedings (Non-Refereed)

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.
2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).
3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

1. *GSM Air Interface Simulator*: Developed a full voice, data and SMS capable simulator for the wireless portion of a GSM network. Models communications down to the timeslot for highest possible accuracy. Used in the majority of our work on cellular security.
2. *Malicious Telephony Load Tester*: Built a system on top of the TM1 Telecom Database testing suite to allow for a comparison of malicious traffic of varying composition.

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.
2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop*, CCSW '20, 2020.
2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.
3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.
4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.
5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.
6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.
7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.

8. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. **SaTC:CORE:Medium: Securing the Voice Processing Pipeline Against Adversarial Audio**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler
Amount: \$1,199,999 over 4 years
Awarded: October 2019
2. **Artus Protocol STTR Phase II**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$800,000 over 4 years
Awarded: August 2019
3. **Evaluating the Security of QR Code-Based Payments**
Sponsor: Discover Financial
Investigator(s): Patrick Traynor (PI)
Amount: \$50,000 over 1 year
Awarded: September 2018
4. **Workshop: Addressing the Technical Security Challenges of Emerging Digital Financial Services**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$50,000 over 1 year
Awarded: September 2017
5. **Designing Strong End-to-End Authentication Mechanisms for Modern Telephony Systems**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded: July 2016
6. **Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem**
Sponsor: National Science Foundation
Investigator(s): Patrick Traynor (PI), Kevin Butler, Shigang Chen
Amount: \$1,200,000 over 4 years
Awarded: June 2016
7. **Evaluating and Improving Security in Emerging Branchless Banking Systems**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded July 2015
8. **Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems**
Sponsor: CISE-ECE Harris Endowed Seed Fund Program

Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)
Amount: \$40,000 over 1 year
Awarded December 2014

9. **Mobile Excursion Study Support**

Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
Amount: \$280,000 over 3 months
Awarded July 2012

10. **Characterizing the Security Limitations of Accessing the Mobile Web**

Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
Amount: \$334,000 over 3 years
Awarded July 2012

11. **Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure**

Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
Amount: \$210,081 over 1 year
Awarded June 2011

12. **Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation**

Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
Amount: \$580,000 over 4 years
Awarded May 2011

13. **Security for Converged IMS Networks**

Sponsor: US Department of Defense
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
Amount: \$242,401 over 1 year
Awarded August 2010

14. **CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones**

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$400,000 over 5 years
Awarded: May 2010

15. **Provably Anonymous Networking Through Secure Function Evaluation**

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$200,000 over 2 years
Awarded: July 2009

16. **Characterizing and Mitigating Device-Based Attacks in Cellular Telecommunications Networks**

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI) and Jonathon Giffin
Amount: \$450,000 over 3 years
Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: \$1,600,000 over 4 years
Awarded May 2019
2. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: \$300,000 for 2 years
Submitted December 2016
3. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: \$532,952 for 2 years
Submitted May 2016
4. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: \$200,000 for 2 years
Submitted: June 2015
5. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: \$500,000 for 3 years
Submitted: December 2012
6. **Facilitating Free and Open Access to Information on the Internet**
Sponsor: NSF Trustworthy Computing
Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
Amount: \$1,500,000 for 4 years
Awarded: June 2011
7. **Monitoring Free and Open Access to Information on the Internet**
Sponsor: Google Focus Program
Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
Amount: \$1,000,000 for 2 years
Awarded: November 2011
8. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
Sponsor: Health Systems Institute (HSI) Seed Grant Program

Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
Amount: \$50,000 over 1 year
Awarded: August 2009

9. **Federal Cyber Service Scholarships at Georgia Tech**

Sponsor: NSF SFS Scholarships
Investigator(s): Seymour Goodman (PI), Patrick Traynor
Amount: \$1,250,682 over 5 years
Awarded: June 2009

10. **Security for IMS-Enabled Converged Applications**

Sponsor: US Department of Defense
Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
Amount: \$146,121 for 1 year
Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

1. Fellow, Center for Financial Inclusion at Accion, 2017.
2. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.
3. Best Paper, The ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec); Budapest, Hungary, 2013.
4. Best Student Paper, The Information Security Conference (ISC); Passau, Germany, 2012
5. Lockheed Inspirational Young Faculty Award, 2012
6. Best Demo, "Is Browsing the Internet on Your Mobile Phone Secure?" Chaitrali Amrutkar (Ph.D Advisee), CoC Research Day, 2011
7. Best Poster, "(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers" Arunabh Verma, Henry Carter (MS, Ph.D Advisees), CoC Research Day, 2011
8. National Science Foundation CAREER Award, 2010
9. Pennsylvania State University Alumni Association Dissertation Award, 2007
10. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
11. AT&T Wireless Fellowship, 2005

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

1. Senior Member, Association for Computing Machinery (ACM)
2. Senior Member, Institute of Electrical and Electronics Engineers (IEEE)
3. Member, USENIX Advanced Computing Systems Association (USENIX)

A.2. Conference Committee Activities

1. Program Chair, *USENIX Security Symposium (SECURITY)*: 2019
2. Program Chair, *Network and Distributed System Security Symposium (NDSS)*: 2017 (co-chair), 2018
3. Program Chair, *USENIX Workshop on Offensive Technologies (WOOT)*: 2016
4. Program Chair, *ACM Conference on Wireless Network Security (WiSec)*: 2014
5. Program Co-Chair, *Annual Computer Security Applications Conference (ACSAC)*: 2012, 2013
6. Program Chair, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2012
7. Chair Invited Talks Committee, *USENIX Security Symposium (SECURITY)*: 2014
8. Workshops Chair, *IEEE Conference on Communications and Network Security (CNS)*: 2016
9. Program Committee, *USENIX Security Symposium (SECURITY)*: 2008, 2009, 2010, 2013, 2015-2018, 2020-2021
10. Program Committee, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2009, 2010, 2011, 2012, 2013, 2014
11. Program Committee, *ACM Conference On Computer and Communications Security (CCS)*: 2009, 2013, 2014, 2015
12. Program Committee, *Network and Distributed System Security Symposium (NDSS)*: 2010, 2013-2016, 2020-2021
13. Program Committee, *IEEE European Symposium on Security and Privacy (Euro S&P)*: 2016
14. Program Committee, *Annual Computer Security Applications Conference (ACSAC)*: 2008, 2009, 2010, 2011, 2015
15. Program Committee, *ACM Conference on Wireless Network Security (WiSec)*: 2009, 2010, 2013, 2015, 2016
16. Program Committee, *International Conference on Financial Cryptography and Data Security (FC)*: 2010, 2013
17. Program Committee, *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*: 2016.
18. Program Committee, *ICST Conference on Security and Privacy in Communication Networks (SecureComm)*: 2009, 2010
19. Program Committee, *Privacy Enhancing Technologies Symposium (PETS)*: 2015, 2016

20. Program Committee, *International World Wide Web Conference (WWW)*: 2016
21. Program Committee, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2011
22. Program Committee, *ACM SIGCOMM Workshop on Networking, Systems, and Applications on Mobile Handhelds (MOBIHELD)*: 2010
23. Program Committee, *International Workshop on Mobile Security (WMS)*: 2010
24. Program Committee, *European Symposium on Research in Computer Security (ESORICS)*: 2009, 2011
25. Program Committee, *IEEE Conference on Mobile Ad-hoc and Sensor Systems (MASS)*: 2009, 2010
26. Program Committee, *Information Security Conference (ISC)*: 2010
27. Program Committee, *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*: 2009
28. Program Committee, *Computer Security Architecture Workshop (CSAW)*: 2008
29. Program Committee, *IWCMC Computer and Network Security Symposium*: 2009
30. Program Committee, *IARIA International Conference on Internet Monitoring and Protection (ICIMP)*: 2009
31. Program Committee, *IEEE Workshop on Network Security and Privacy (NSP)*: 2008
32. Program Committee, *IEEE International Workshop on Wireless and Sensor Networks Security (WSNS)*: 2008, 2009
33. Program Committee, *IEEE Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC)*: 2008
34. Program Committee, *ACM Conference on Computer and Communications Security, Industry and Government Track (CCS I&G)*: 2006, 2007
35. Program Committee, *Workshop on Secure Network Protocols (NPsec)*: 2006
36. Program Committee, *International Conference on Information Systems Security (ICISS)*: 2006, 2009, 2010
37. Program Committee, *IEEE LCN Workshop on Network Security (WNS)*: 2006, 2007, 2008

B. On-Campus Committees

B.1. University of Florida

1. Member, Computer and Information Science and Engineering Steering Committee, 2015-2017.
2. Member, Graduate Recruiting Committee, 2015-2017.
3. Chair, Computer and Information Science and Engineering Industrial Advisory Board, 2014-2015.

B.2. Georgia Tech

1. Member, Massive Open Online Master's (MOOMS) Investigation Committee, 2012-2013.
2. Chair, School of Computer Science Ph.D. Review Committee, 2012.
3. Member, School of Computer Science Ph.D Review Committee, 2011.
4. Faculty Advisor, Grey H@T - Georgia Tech Undergraduate Security Club, 2011-2014.
5. Member, School of Computer Science Ph.D. Review Committee, 2011.
6. Member, School Advisory Committee, School of Computer Science, 2011-2013.
7. Member, School of Computer Science Chair Recruiting Committee, 2011.
8. Member, School of Computer Science Faculty Recruiting Committee, 2010, 2011.
9. Chair, College of Computing Ph.D. Welcome Weekend Committee, 2009, 2010, 2011 (co-chair).
10. Member, College of Computing Ph.D. Recruiting Committee, 2009.
11. Member, Georgia Tech Computer and Network Usage Security Policy (CNUSP) Evaluation Group, 2009.

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, University of Florida, Summer 2017.
Advisor: Professor Patrick Traynor.
2. Adam Bates, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
Advisor: Professor Kevin Butler.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
Advisor: Professor Kevin Butler.
4. Henry Carter, College of Computing, Georgia Tech, Fall 2015.
Advisor: Professor Patrick Traynor.
5. David Dewey, College of Computing, Georgia Tech, Fall 2015.
Advisor: Professor Patrick Traynor.
6. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2014.
Advisor: Professor Umakishore Ramachandran.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Summer 2013.
Advisor: Professor Patrick Traynor.
8. Long Lu, College of Computing, Georgia Tech, Summer 2013.
Advisor: Professor Wenke Lee.

9. Manos Antonakakis, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Wenke Lee.
10. Junjie Zhang, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Wenke Lee.
11. Italo Dacosta, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Patrick Traynor.
12. Virendra Kumar, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Alexandra Boldyreva.
13. Anirudh Ramachandran, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Nick Feamster.
14. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Mustaque Ahamad.
15. Kapil Singh, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Wenke Lee.
16. Abhinav Srivastava, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Jon Giffin.
17. Adam O'Neill, College of Computing, Georgia Tech, Summer 2010.
Advisor: Professor Alexandra Boldyreva.
18. David Cash, College of Computing, Georgia Tech, Fall 2009.
Advisor: Professor Alexandra Boldyreva.

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

1. Shannon Eggers, Department of Materials Sciences and Engineering - Nuclear Engineering Program, University of Florida, Fall 2016.
Advisor: Professor Kelly Jordan.
2. Ed Carlisle, Department of Electrical and Computer Engineering, University of Florida, Summer 2016.
Advisor: Professor Alan George.
3. Claudio Marforio, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Fall 2015.
Advisor: Professor Srdjan Capkun.
4. Nils Ole Tippenhauer, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Spring 2012.
Advisor: Professor Srdjan Capkun.
5. Bongkyoung Kwon, School of Electrical and Computer Engineering, Georgia Tech, Summer 2009.
Advisor: Professor John Copeland.

Ph.D. Thesis Proposal Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, Spring 2016.
Advisor: Professor Patrick Traynor.
2. Maliheh Shirvanian, University of Alabama, Birmingham, Spring 2016.
Advisor: Professor Nitesh Saxena.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, Fall 2015.
Advisor: Professor Kevin Butler.
4. Adam Bates, Department of Computer and Information Science and Engineering, Fall 2015.
Advisor: Professor Kevin Butler.
5. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Umakishore Ramachandran.
6. Long Lu, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2012.
Advisor: Professor Patrick Traynor.
8. Junjie Zhang, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
9. Italo Dacosta, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
10. Manos Antonakakis, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
11. Abhinav Srivastava, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Jon Giffin.
12. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mustaque Ahamad.
13. Kapil Singh, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Wenke Lee.
14. Anirudh Ramachandran, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
15. Adam O'Neill, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Alexandra Boldyreva.
16. David Cash, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.

Ph.D. Qualifying Exam Committees—Georgia Tech

1. Byoungyoung Lee, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
2. Yizheng Chen, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professors Mustaque Ahamad and Roberto Perdesi.
7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Jon Giffin.
10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Alex Orso.
15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Patrick Traynor.
16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Wenke Lee and Professor Jon Giffin.
17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.
19. Partha Kanuparth, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Constantine Dorvolis.
20. Long Lu, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Wenke Lee.
21. Virendra Kumar, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.
22. Frank Park, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Patrick Traynor.

23. Italo Dacosta, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Mustaque Ahamad and Professor Patrick Traynor.
24. Adam O'Neill, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Alexandra Boldyreva.

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

1. Skim Reaper, *Co-Founder and CEO*, 2019-Present.
2. CryptoDrop Anti-Ransomware, *Co-Founder and CEO*, 2017-2018.
3. Pindrop Security, *Research Fellow and Co-Founder*, Spring 2012 - Spring 2014.
4. United States Army (via US Falcon), *Information Assurance Officer Training Program*, Spring 2010.
5. 3G Americas, *Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Systems*, Fall 2008.

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

1. Fellow, Kavli Foundation, 2017.
2. Fellow, Center for Financial Inclusion at Accion, 2016.
3. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.

B. Invited Conference Session Chairmanships

1. Session Chair, *Work-in-Progress* at the *USENIX Security Symposium (SECURITY)*, 2016.
2. Session Chair, *Mobile Security* at the *USENIX Security Symposium (SECURITY)*, 2013.
3. Poster Chair, *USENIX Security Symposium (SECURITY)*, 2010, 2011.
4. Session Chair, *Privacy and Anonymity* at the *USENIX Workshop on Hot Topics in Security (HotSec)*, 2011.
5. Session Chair, *Security of Authentication and Protection Mechanisms* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2011.
6. Session Chair, *Information Abuse* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2010.
7. Session Chair, *RFID Security* at the *ACM Conference on Computer and Communications Security (CCS)*, 2009.
8. Session Chair, *Browser Security Session* at the *USENIX Security Symposium (SECURITY)*, 2009.
9. Session Chair, *Information Security Session* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
10. Session Chair, *Work-in-Progress* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
11. Session Chair, *Work/Opinions-in-Progress* at the *ISOC Network and Distributed Systems Security (NDSS) Symposium*, 2009.
12. Session Chair, *Privacy Session* at the *USENIX Security Symposium (SECURITY)*, 2008.

C. Professional Registration

None.

D. Patents

1. Walter Nolen Scaife, Patrick G. Traynor and Christian Peeters, "Payment Card Overlay Skimmer Detection", United States Patent # 10,496,914, Filed October 2017, Issued December 2019. (See also # 10,936,928)
2. Patrick G. Traynor, David P. Arnold, Walter Nolen Scaife, Christian Peeters, and Camilo Valez Cuervo, "Detecting counterfeit magnetic stripe cards using encoding jitter", United States Patent # 10,803,261, Filed May 2017, Issued October 2020.
3. Patrick G. Traynor, Bradley Reaves, Logan Blue, Luis Vargas, Hadi Abdullah, and Thomas Shrimpton, "Identity and content authentication for phone calls", United States Patent # 10,764,043, Filed Apr 2017, Issued September 2020.

4. Walter Nolen Scaife, Henry Carter, Patrick G. Traynor and Kevin R. B. Butler. "Malware Detection Through User Data Transformation Monitoring", United States Patent # 10,685,114. Filed September 2015, Issued June 2020.
5. Vijay A. Balasubramaniyan, Mustaque Ahamad, Patrick G. Traynor. "Using Single-Ended Audio Features to Automatically Determine Voice Call Provenance", United States Patent, #9,037,113 June 2010, Issued May 2015. (See also #9,516,497 and #10,523,809)
6. Patrick G. Traynor, Byungsuk Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

- *ACM Transactions on Information and System Security (TISSEC)* 2015-present

Guest Editor:

Journals

- *IEEE Security and Privacy Magazine (S&P)* 2013

Reviewer for:

Journals

- *ACM Transactions on Information and System Security (TISSEC)* 2008, 2009, 2010, 2011, 2012, 2013
- *IEEE Transactions on Dependable and Secure Computing (TDSC)* 2012, 2013
- *IEEE Security and Privacy Magazine (S&P)* 2010, 2011
- *Communications of the ACM (CACM)* 2010
- *Journal of Anesthesia & Analgesia* 2009
- *IEEE Transactions on Mobile Computing (TMC)* 2008, 2010, 2011, 2012, 2013
- *IEEE Transactions on Internet Technology (TOIT)* 2009, 2010
- *ACM Mobile Computing and Communications Review (MC2R)* 2008
- *IEEE/ACM Transactions on Networking (TON)* 2007, 2008
- *Journal of Pervasive and Mobile Computing (PMC)* 2009, 2010
- *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 2005, 2009, 2010
- *IEEE Transactions on Computers (TOC)* 2010
- *Journal of Security and Communication Networks (SCN)* 2008
- *IEEE Communications Letters (CL)* 2007, 2009
- *IEEE Transactions on Wireless Communications (TWC)* 2007
- *Pervasive and Mobile Computing (PMC)* 2007

- *IEEE Transactions on Software Engineering (TSE)* 2007, 2008
- *Journal of Wireless Networks (WiNet)* 2006, 2007, 2008, 2009
- *Journal of Wireless Communications and Mobile Computing* 2006
- *ACM Computing Surveys (ACMCS)* 2006
- *Information Processing Letters (IPL)* 2006
- *IEEE Transactions on Very Large Scale Integration Systems (TVLSIS)* 2006

Conferences and Workshops

- *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2011
- *ACM Conference on Computer and Communications Security (CCS)*, 2008, 2011
- *IEEE Symposium on Security and Privacy (OAKLAND)* 2007, 2008
- *Computer Security Foundations (CSF)*, 2011
- *IFIP Conference on Data and Applications Security (DBSec)* 2008
- *Financial Cryptography (FC)* 2007, 2008
- *International Conference on VLSI Design (VLSI)* 2007
- *Annual Computer Security Applications Conference (ACSAC)* 2005, 2006, 2007
- *USENIX Workshop on Hot Topics in Security (HotSec)* 2007
- *International Conference on Information Systems Security (ICISS)* 2007
- *IEEE International Conference on Computer Engineering & Systems (ICCES)* 2007
- *International Workshop on Security (IWSec)* 2006, 2007
- *USENIX Security Symposium (SECURITY)* 2006, 2007
- *IEEE Sarnoff Symposium (SARNOFF)* 2007
- *International Conference on New Technologies, Mobility and Security (NTMS)* 2007
- *IEEE Infocom (INFOCOM)* 2007
- *Network and Distributed System Security Symposium (NDSS)* 2007
- *International Workshop on Storage Security and Survivability (IWSSS)* 2006
- *ACM Conference on Computer and Communications Security (CCS)* 2006
- *IEEE GLOBECOM (GLOBECOM)* 2006
- *International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS)* 2006
- *IFIP Conference on Data and Applications Security (DBSec)* 2006
- *Emerging Trends in Information and Communications Security (ETRICS)* 2006
- *International Conference on Applied Cryptography and Network Security (ACNS)* 2006

- *ACM Symposium on Access Control Models and Technology (SACMAT)* 2006
- *IEEE Conference on Communication Systems Software & Middleware (COMSWARE)* 2006
- *International Conference on Cryptology in India (IndoCrypt)* 2005
- *IEEE Symposium on New Frontiers in Dynamic Spectrum Access (DySPAN)* 2005
- *European Symposium on Research in Computer Security (ESORICS)* 2005

F. Expert Witness Services

1. *Apple/Microsoft vs. Zipit Wireless*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Submitted to PTAB. *May 2021 - Ongoing*.
2. *Blackberry Inc v MobileIron, Inc*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Case settled. *January 2021 - March 2021*.
3. *Apple Inc v Seven Networks, LLC*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Three of four petitions instituted by PTAB. Fourth rejected via discretion, case settled. *August 2019 - November 2020*.
4. *mSIGNIA, Inc. v. InAuth, Inc.*: Expert Witness for the Defense for Inter Partes Review, Non-Infringement and Invalidity (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018*.
5. *Huawei v. T-Mobile*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017*.
6. *Ericsson v Apple*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015*.
7. *Mayfonk v Nike*: Expert Witness for the Plaintiff for Infringement (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015*.
8. *Maxim Integrated Products v Bank of the West*: Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). Verdict: Dismissed with prejudice. *January 2014 - August 2014*.
9. *Maxim Integrated Products v Comerica Inc, et al*: Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). Verdict: Settled. *June 2014 - August 2014*.
10. *William Grecia v. Apple Inc. et al*: Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). Verdict: Closed in initial pleadings, dismissed with prejudice. *July 2014 - August 2014*.
11. *Intertrust Technologies Corp. v. Apple Inc.*: Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). Verdict: Settled. *October 2013 - February 2014*.
12. *Maxim Integrated Products v KeyCorp Bank*: Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) Verdict: Settled. *April 2013 - June 2013*.
13. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015*.

V. OTHER CONTRIBUTIONS

A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)

1. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
2. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. North Carolina State University Department of Computer Science Colloquium, January 2020. Raleigh, NC.
3. Moving from research to practice: How to maximize the impact of SaTC projects. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) PI Meeting, October 2019. Alexandria, VA.
4. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Purdue University Computer Science Excellence Lecture Series, October 2019. West Lafayette, IN.
5. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.
6. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. CISPA – Helmholtz Center for Information Security, Saarland University, February 2019. Saarbrücken, Germany.
7. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.
8. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
9. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweden.
10. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
11. Why Caller-ID Spoofing Is So Easy (and Why End-To-End Solutions Are the Way Forward). IEEE Workshop on Technology and Consumer Protection (ConPro'18), May 2018. San Francisco, CA.
12. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
13. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.
14. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
15. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
16. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
17. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.

18. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
19. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
20. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. KAIST Information Security Seminar - Korean Advanced Institute of Science and Technology, June 2016. Daejeon, South Korea.
21. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.
23. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.
24. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.
25. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.
26. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
27. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
28. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
29. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
30. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
31. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.
32. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2013. Belfast, Northern Ireland.
33. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.
34. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.
35. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.

36. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.
37. Chasing Telephony Security: Where the Wild Things... Are? University of Washington Department of Electrical Engineering, Network Security Lab (NSL): Invited Talk, November 2012. Seattle, WA.
38. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.
39. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.
40. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.
41. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.
42. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.
43. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.
44. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.
45. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.
46. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.
47. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.
48. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.
49. Privacy and Security Concerns for Personal and Mobile Health Devices. Invited Talk: Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies, October 2009. Indianapolis, IN.
50. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.
51. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.
52. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.
53. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.
54. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.
55. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.

56. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.
57. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.
58. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.
59. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.
60. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.
61. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.
62. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.
63. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.
64. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.
65. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.
66. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.
67. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
68. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

B. Special Activities

Presentations to Lay Media

1. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie <https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/>, July 2016.
2. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - <http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255>, July 2016.
3. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
4. Ransomware 'stopped' by new software. BBC - <http://www.bbc.com/news/technology-36772461>, July 2016.

5. Researchers create effective anti-ransomware solution. Help Net Security - <https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/>, July 2016.
6. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.
7. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
8. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - <http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/>, July 2016.
9. Desarrollan una solución para detener el ransomware. ComputerHoy - <http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972>, July 2016.
10. Why your antivirus software can't stop ransomware. Futurity - <http://www.futurity.org/ransomware-computer-files-1198242-2/>, July 2016.
11. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - <http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml>, July 2016.
12. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - <https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomware-threat-071116.html>, July 2016.
13. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - <http://phys.org/news/2016-07-extortion-extinction-ransomware.html>, July 2016.
14. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - <https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem>, July 2016.
15. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured - Researchers. <http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/>, August 2015.
16. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. <http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmSQ.twitter>, August 2015.
17. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>, August 2015.
18. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. <http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198>, December 2013.

19. N. V. The Economist - The Threat in the Pocket. <http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket>, October 2013.
20. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. <http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move>, October 2013.
21. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. <http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399>, October 2013.
22. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.
23. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. <http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/>, June 2013.
24. Jim Burrell. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.
25. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. <http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html>, December 2012.
26. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. <http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999>, December 2012.
27. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. <http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html>, December 2012.
28. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuId, December 2012.
29. Suzanne Choney. Mobile browser woes can fool even experts: report. <http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203>, December 2012.
30. Meghan Kelly. VentureBeat - 3 hot security startups to watch. <http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/>, February 2012.
31. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. <http://www.gsnmagazine.com/node/25721?c=communications>, February 2012.
32. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.

33. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - <http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html>, October 2011.
34. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - <http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing>, October 2011.
35. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
36. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - <http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx>, October 2011.
37. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html>, October 2011.
38. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.
39. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - <http://www.popsoci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks>, October 2010.
40. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.
41. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. <http://www.sciencedaily.com/releases/2010/10/101005121820.htm>, October 2010.
42. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.
43. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - <http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies-iphone-users-cripple-att/story?id=9355447>, December 2009.
44. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - http://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.
45. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - <http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html>, November 2009.
46. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - <http://www.scmagazineus.com/remote-repair-for-infected-phones-in-development/article/157504/>, November 2009.

47. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - <http://www.networkworld.com/news/2009/111109-smartphone-security-georgia-tech.html?hpg1=bn>, November 2009.
48. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - <http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html>, November 2009.
49. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11/2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.
50. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - <http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3>, July 2009.
51. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - <http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/>, June 2009.
52. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - <http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/>, June 2009.
53. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - <http://www.uwire.com/Article.aspx?id=3738798>, February 2009.
54. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - <http://www.npr.org/templates/story/story.php?storyId=99790788>, January 2009.
55. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.
56. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - <http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml>, October 2008.
57. Associated Press. Hackers Expected To Start Targeting Cell Phones. <http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html>, 2008.
58. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college-campus_alerts.html, 2008.
59. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.
60. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.
61. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas <http://www.3gamericas.org/English/newsroom/DisplayPressRelease.cfm?id=3400&s=ENG>, 2008.
62. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - <http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx>, 2008.

63. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine <http://www.slate.com/id/2161402/>, 2007.
64. Jamming Cellphones with Text Messages. Slashdot <http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>, 2005.
65. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.
66. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times <http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss>, 2005.