IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Graham Merrett	
U.S. Patent No.:	8,918,127	Attorney Docket No. 50095-0260IP1
Issue Date:	December 23, 2014	
Application No.:	13/762,347	
Filing Date:	February 7, 2013	
Title:	MESSAGING SERVICE IN A WIRELESS COMMUNICATIONS NETWORK	

DECLARATION OF DR. PATRICK TRAYNOR

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 under Section 1001 of Title 18 of the United States Code.

Date: 29 August 2025

By: _____
Patrick Traynor, Ph.D.

Table of Contents

I. QUALIFICATIONS AND BACKGROUND INFORMATION.....3

II. LEGAL PRINCIPLES.....9

A. Anticipation.....9

B. Obviousness.....10

III. OVERVIEW OF CONCLUSIONS FORMED.....11

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '127 PATENT11

V. INTERPRETATIONS OF THE '127 PATENT CLAIMS AT ISSUE.....12

VI. THE '127 PATENT.....12

A. Overview of the '127 Patent.....12

B. Prosecution History of the '127 Patent.....14

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES..15

A. Overview of Horvath.....15

B. Overview of Tsampalis.....20

C. Combination of Horvath and Tsampalis.....26

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '127 CLAIMS UNPATENTABLE.....37

A. The Horvath-Tsampalis Combination Renders Claims 1-20 Obvious.....37

IX. CONCLUSION.....103

DECLARATION OF DR. PATRICK TRAYNOR

I, Patrick Gerard Traynor, of Gainesville, Florida, declare that:

I. QUALIFICATIONS AND BACKGROUND INFORMATION

1. My name is Patrick Gerard Traynor and I have been retained as an expert witness by Apple in the matter of., Apple Inc. ("Apple") vs. HBCU Messaging US LP. My qualifications for forming these conclusions are summarized below.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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).

7. 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.

8. 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.

9. 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).

10. 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).

11. 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).

12. 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).

13. I am a named inventor on more than 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.

14. My curriculum vitae, included with this declaration 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.

15. In writing this Declaration, I have considered the following: my own knowledge and experience, including my work experience in mobile systems and networks; my experience in teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed the following publications and materials, in addition to other materials I cite in my declaration:

- APPLE-1001 U.S. Patent No. 8,918,127 (“the ’127 Patent”)
- APPLE-1002 File History of U.S. Patent No. 8,918,127
- APPLE-1004 U.S. Pub. No. 2007/0254681 (“Horvath”)
- APPLE-1005 U.S. Pub. No. 2004/0203956 (“Tsampalis”)
- APPLE-1007 Chatterjee et al., “Instant Messaging and Presence Technologies for College Campuses.” IEEE Network, May/June 2005. (“Chatterjee”)
- APPLE-1008 U.S. Pub. No. 2005/0243978 (“Son”)
- APPLE-1009 UK Pub. No. 2432482 (“Beaumont”)
- APPLE-1010 U.S. Patent No. 9,408,077 (“David”)
- APPLE-1011 U.S. Patent No. 6,940,844 (“Purkayastha”)
- APPLE-1012 U.S. Patent No. 7,702,342 (“Duan”)
- APPLE-1013 U.S. Patent No. 8,819,145 (“Gailloux”)
- APPLE-1014 U.S. Pub. No. 2006/0286984 (“Bonner”)
- APPLE-1015 U.S. Pub. No. 2005/0197142 (“Major”)
- APPLE-1016 U.S. Pub. No. 2005/0037762 to Gurbani et al. (“Gurbani”)
- APPLE-1017 U.S. Patent No. 9,167,401 to Helferich (“Helferich”)
- APPLE-1018 U.S. Patent No. 6,430,604 (“Ogle”)
- APPLE-1019 PCT Pub. No. WO 2006/029331 (“Henderson”)

- APPLE-1020 U.S. Patent No. 7,236,472 ("Lazaridis")
- APPLE-1021 U.S. Patent No. 8,006,190 ("Quoc")
- APPLE-1022 U.S. Patent No. 6,678,524 ("Hansson")
- APPLE-1023 U.S. Pub. No. 2006/0056309 ("Maaniitty")
- APPLE-1024 U.S. Patent No. 7,171,190 ("Ye")
- APPLE-1025 Qi et al., 2004, July. "Multimedia Messaging Service." Available at https://www.zte.com.cn/global/about/magazine/zte-communications/2004/1/en_68/162264.html ("Qi")
- APPLE-1036 International Pub. No. WO 2007/052264 ("Agiv")
- APPLE-1037 T-Mobile webpage https://www.t-mobile.com/home-internet/the-signal/internet-help/the-complete-wifi-history
- APPLE-1038 U.S. Pub. No. 2010/0009704 ("Fan")
- APPLE-1039 U.S. Pub. No. 2004/0087305 ("Jiang")
- APPLE-1040 U.S. Pub. No. 2007/0178895 ("Bot")
- APPLE-1041 Kumar et al., Special Delivery: An Increase in MMS Adoption, IEEE Potentials (January/February 2009)
- APPLE-1042 Brugge, MSS-Multimedia Messaging and MMS-Interconnection, ECC Report 62 (November 2004)
- APPLE-1043 U.S. Pub. No. 2008/0176538 ("Terrill")

- APPLE-1100 Complaint, *HBCU Messaging US LP v. Apple, Inc. et al.*, 1-24-cv-01199 (WDTX) (Oct. 7, 2024)
- APPLE-1101 Infringement Charts of the '127 Patent

II. LEGAL PRINCIPLES

A. Anticipation

16. I have been informed that a patent claim is invalid as anticipated under 35 U.S.C. § 102 if each and every element of a claim, as properly construed, is found either explicitly or inherently in a single prior art reference. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

17. I have been informed that a claim is invalid under 35 U.S.C. § 102(a) if the claimed invention was known or used by others in the U.S., or was patented or published anywhere, before the applicant's invention. I further have been informed that a claim is invalid under 35 U.S.C. § 102(b) if the invention was patented or published anywhere, or was in public use, on sale, or offered for sale in this country, more than one year prior to the filing date of the patent application (critical date). And a claim is invalid, as I have been informed, under 35 U.S.C. § 102(e), if an invention described by that claim was described in a U.S. patent granted on an application for a patent by another that was filed in the U.S. before the date of invention for such a claim.

B. Obviousness

18. 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 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: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others. For purposes of my analysis, and at the direction of counsel, I have applied the July 24, 2007 filing date of the Australian Patent Application No. 2007903979 listed on the face of the '127 Patent as the date of invention in my obviousness analyses, although in many cases the same analysis would hold true even at an earlier time than July 24, 2007.

19. 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 to modify the single prior art reference, or combine two or more references, in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or

references themselves, the knowledge or "common sense" of one skilled in the art, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole. I have been informed that 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.

III. OVERVIEW OF CONCLUSIONS FORMED

20. This expert Declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions, based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-20 of the '127 Patent are obvious over Horvath in view of Tsampalis.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '127 PATENT

21. Based on the foregoing and upon my experience in this area, a person of ordinary skill in the art ("POSITA") relating to the subject matter of the '127 Patent by the Critical Date (July 24, 2007) would have had at least a bachelor's degree in computer science, electrical engineering, computer engineering, or a related field, with 2-3 years of industry experience in computer networking and wireless telecommunications. Additional graduate education could substitute for professional experience, and vice versa.

22. Based on my experiences, I have a good understanding of the capabilities of a POSITA as I was such an individual at the time of the Critical Date. Moreover, I have taught, participated in organizations, and worked closely with many such persons over the course of my career.

V. INTERPRETATIONS OF THE '127 PATENT CLAIMS AT ISSUE

23. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). I have been informed by counsel for the Petitioner that I should use July 24, 2007 as the point in time for claim interpretation purposes.

VI. THE '127 PATENT

A. Overview of the '127 Patent

24. The '127 Patent describes techniques for messaging over wireless networks in which a sending wireless device selects a transmission mode for sending an outgoing message based on information indicating whether an intended recipient of the message is a subscriber of a service for receiving messages via a

packet-switched bearer. APPLE-1001, 2:43-3:12, 7:36-9:35, Abstract. The Abstract summarizes the disclosed techniques as follows, for example:

> A method of providing a message service in a sender's wireless device is disclosed. The sender's wireless device may be capable of sending messages via a packet switched base station in a first mode, or via a short message service (SMS) base station that is independent of the packet switched base station, in a second mode. The sender's wireless device determines whether a destination address corresponds to a subscriber of a service for receiving the outgoing message via a packet switched bearer. The sender's wireless device sends, if the destination address corresponds to a subscriber of the service, the outgoing message to the recipient's wireless device via the packet switched base station in the first mode. If the destination address does not correspond to a subscriber of the service, the outgoing message may be sent via the SMS base station in the second mode.

APPLE-1001, Abstract.

25. FIG. 3 is a flowchart that illustrates an example process for selecting a transmission mode for an outgoing message based on information about the recipient:

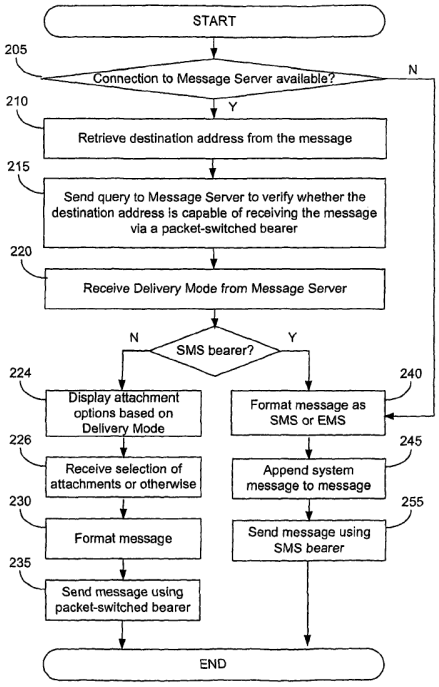


FIG. 3

APPLE-1001, FIG. 3

B. Prosecution History of the '127 Patent

26. In the only Office Action to issue during prosecution, the Examiner rejected[1] application claims 28 and 34-35 as obvious based on Hansson (APPLE-1022) in view of Maaniitty (APPLE-1023) and Ye (APPLE-1024). APPLE-1002, 63-67. The Examiner identified dependent claims 29-33 and 36-39 as allegedly reciting allowable subject matter. *Id.* Applicant responded by cancelling the

[1] The Examiner also issued double patenting rejection for application claims 28-39 based on U.S. Patent No. 8,401,576, which Applicant addressed by filing a terminal disclaimer over the '576 Patent. APPLE-1002, 30-31, 48, 63-67.

rejected claims and adding new independent claims 50 and 60 to include subject matter from certain ones of the allowable dependent claims. APPLE-1002, 47-49.

27. The Examiner issued a notice of allowance following the Applicant's response to the Office Action. APPLE-1002, 3-5. However, as discussed in §VIII, the application never should have been allowed. All features recited in the Challenged Claims are disclosed in one or more of Horvath and Tsampalis, and the claimed combinations of these features would have been obvious before the Critical Date.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Horvath

28. Horvath discloses a method and system for "transmitting short message service messages" with "a wireless device" over "a packet data network 102 and a circuit services network 104." *See e.g.*, APPLE-1004, Title, [0001]-[0002], [0007], [0024]-[0026], [0033], FIGS. 1, 2. Horvath's wireless device (*e.g.*, "wireless device 106") is "a dual mode device capable of communicating on either the packet data network 102 or the circuit services network 104," "based on [a] registration status of the wireless device." APPLE-1004, [0007]-[0008], [0024], [0061], FIGS. 1 (below), 2, 4.

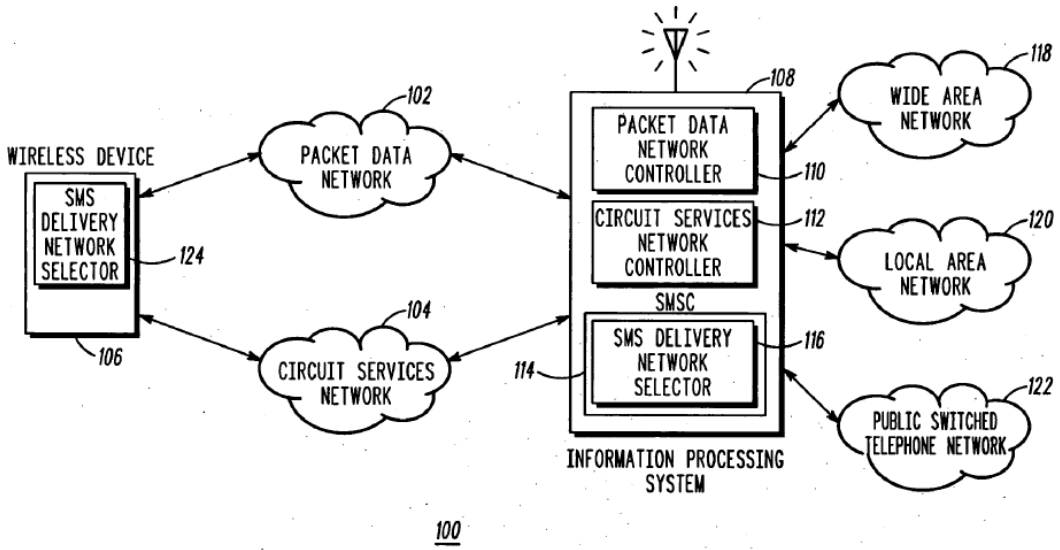


FIG. 1

APPLE-1004, FIG. 1

29. As shown in FIG. 1, wireless device 106 can function both as a sender device that sends messages destined for remote recipient device(s) and as a recipient device that receives message(s) sent from remote sender device(s). When wireless device 106 is instructed to send an SMS message (operating as a sender device), "the wireless device 106 first determines if it [*i.e.*, the sending wireless device] is registered on the packet data network 102," and based on this determination, an "SMS delivery network selector 124" residing on the wireless device 106 "selects a network 102, 104 for the wireless device 106 to transmit [the] SMS message on." APPLE-1004, [0050], [0062] ("[I]f the wireless device 106 is registered on the packet data network 102, the SMS delivery network selector 124 selects the packet data network 102 for transmission of the SMS message. If the

wireless device is not registered on the packet data network 102, the SMS delivery network selector 124 selects the circuit services network 104 for transmission of the SMS message."), [0078], FIGS. 1, 4, 7.

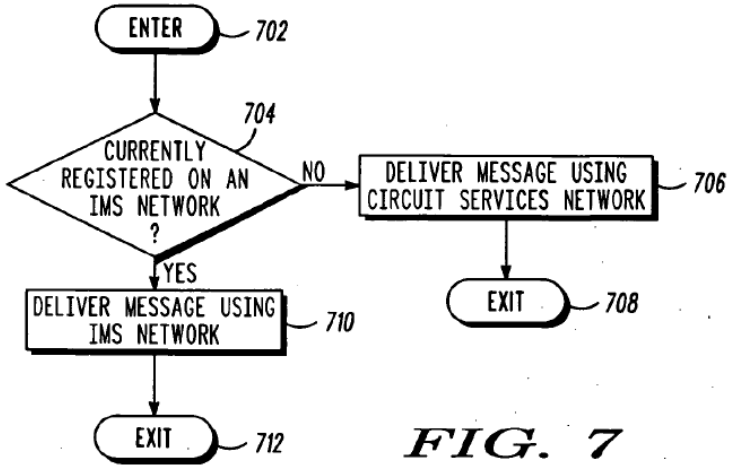


FIG. 7

APPLE-1004, FIG. 7 (Sender Device Perspective)

30. Although Horvath focuses on the selective use of packet switched or circuit switched bearers for delivery of SMS messages, Horvath notes that wireless device 106 can transmit other types of messages as well, including enhanced messaging service ("EMS") messages, multimedia service ("MMS") messages, and instant messages ("IM"). APPLE-1004, [0025], [0038]-[0039] ("An IMS system also includes application servers that host and execute services for the wireless device 106. A service for example, is SMS, MMS, …and the like."). A session initiation protocol ("SIP") network operates atop the packet data network 102 to establish communication sessions and carry encapsulated SMS messages between wireless devices and a server when the circuit switched network 104 is not

used. *Id.* [0041], [0033] ("The SIP network is used for establishing instant messaging, … and other real-time communications over the Internet."), [0050], FIG. 5.

31. When a message is requested to be sent to a wireless device (e.g., wireless device 106) in Horvath's system, the message request is first routed to a server system (e.g., information processing system 108) including a "Short Message Service Center ('SMSC' [114])." APPLE-1004, [0045]-[0047], FIGS. 1-2. SMSC 114 includes an "SMS delivery network selector 116" that "selects either the packet data network 102 or the circuit services network 104 for delivery of a SMS message" based on whether the intended recipient of the message is currently registered on the packet data network 102. *Id.*, [0053], FIG. 3; *see also id.*, [0028], [0045]-[0047], FIGS. 1-2. SMSC 114, with SMS delivery network selector 116, determines the registration status of the recipient wireless device by checking whether the recipient is currently registered with an SIP network on the packet data network 102.[2] *Id.*, Abstract, [0002], [0006], [0008], [0028], [0033]-[0038], [0075]-

[2] The SIP network is supported by an "Internet Protocol multimedia subsystem" (IMS) core and is capable of transmitting rich **multimedia** data. APPLE-1004, [0034]; *see also* APPLE-1012 (describing IMS networks in further detail).

[0076], FIGS. 1, 2, 3, 6. By delivering messages to wireless devices over a packet data network rather than a circuit switched network when a recipient device is registered with the packet data network, Horvath's system reduces the amount of traffic transmitted over the circuit switched network, thereby freeing bandwidth for voice calls or other services on the circuit switched network. APPLE-1004, [0009], [0021], [0039], [0050].

32. FIG. 6 is a flowchart that illustrates "an exemplary process of a SMSC selecting either a circuit services network or a packet data network for delivery of a SMS message to a wireless device" (APPLE-1004, [0016]):

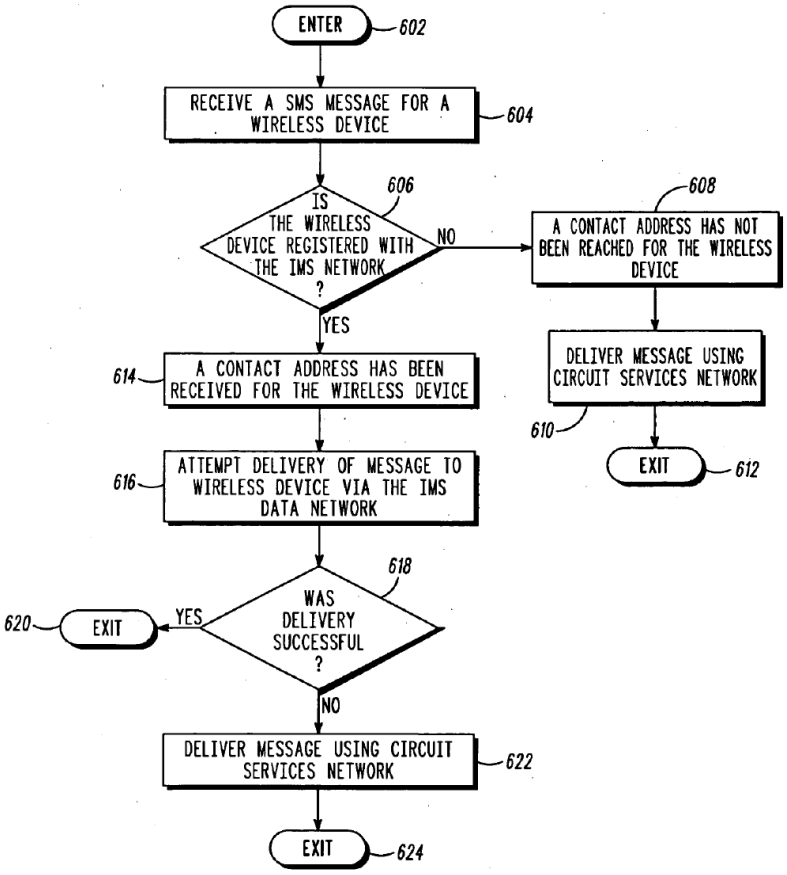


FIG. 6

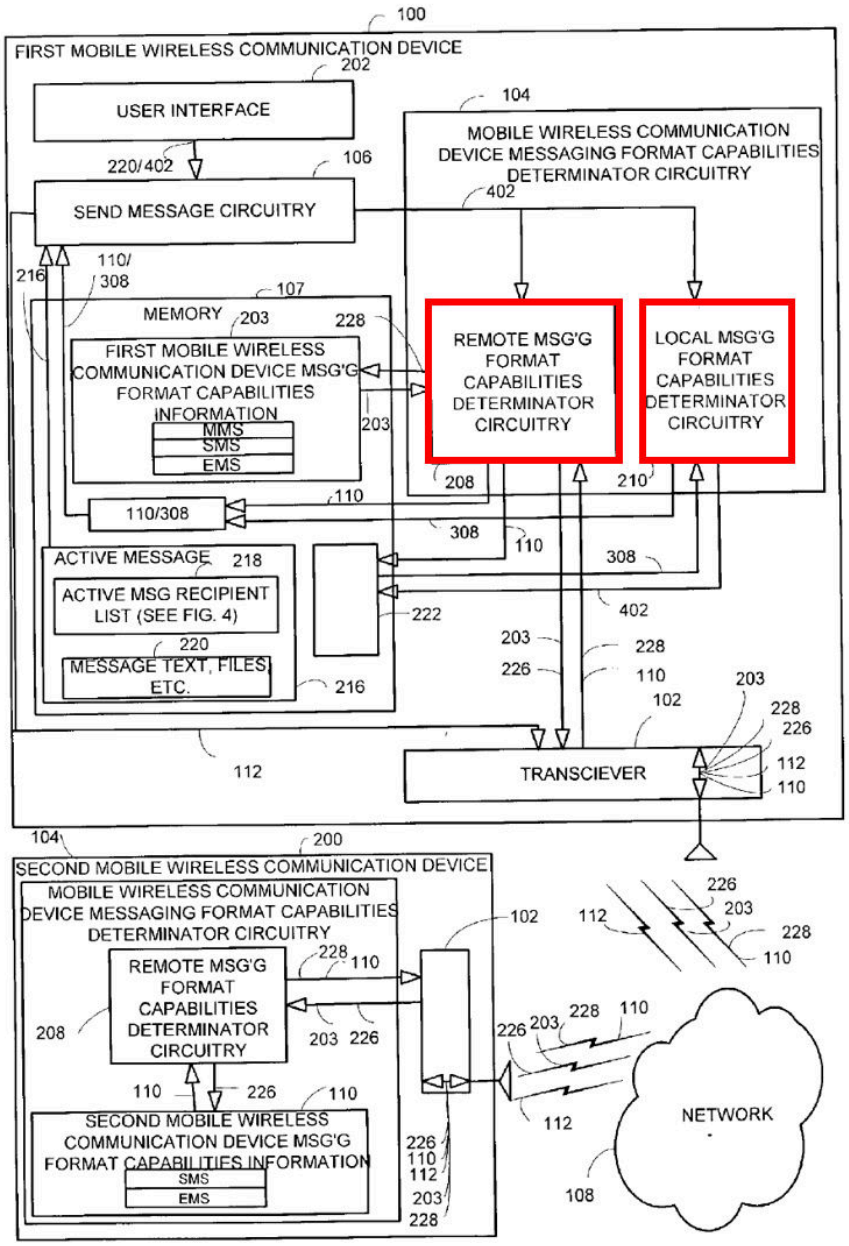
APPLE-1004, FIG. 6 (Server Perspective)

B. Overview of Tsampalis

33. Tsampalis describes a "method and apparatus for providing wireless messaging" in which a first mobile wireless communication device 100 (*i.e.*, a sender device) obtains, either locally or via "a web server" or other "network element," "messaging format capabilities information 110" of a second mobile wireless communication device 200 (*i.e.*, a recipient device) before the sender device sends a message. *See e.g.*, APPLE-1005, Title, Abstract, [0029]-[0039],

FIGS. 1, 2 (below, highlighting the local and remote messaging format capabilities determinator circuitries residing on the first wireless device), 5-7. The messaging format capabilities information 110 (MFCI) indicates the types of messages (*e.g.*, SMS, MMS, EMS) that the intended recipient device is capable of processing. APPLE-1005, [0022]-[0024].

FIG. 2



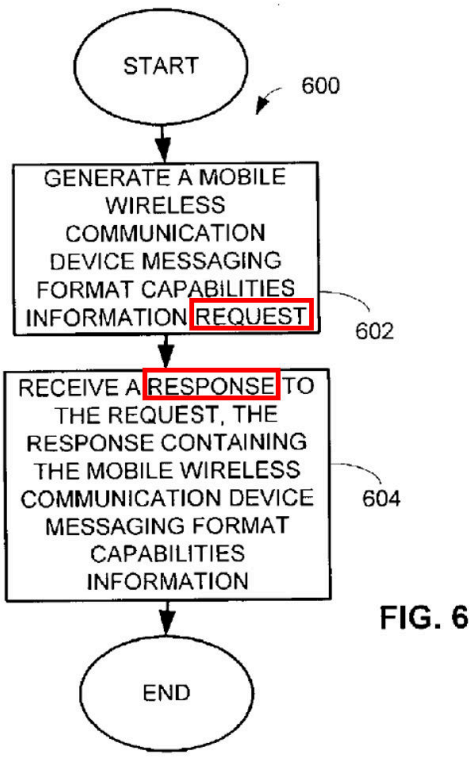
APPLE-1005, FIG. 2 (Annotated)

34. According to Tsampalis, when recipient device 200's format capabilities information 110 "must be retrieved remotely," the sender device 100 generates and sends a "mobile wireless communication device messaging format

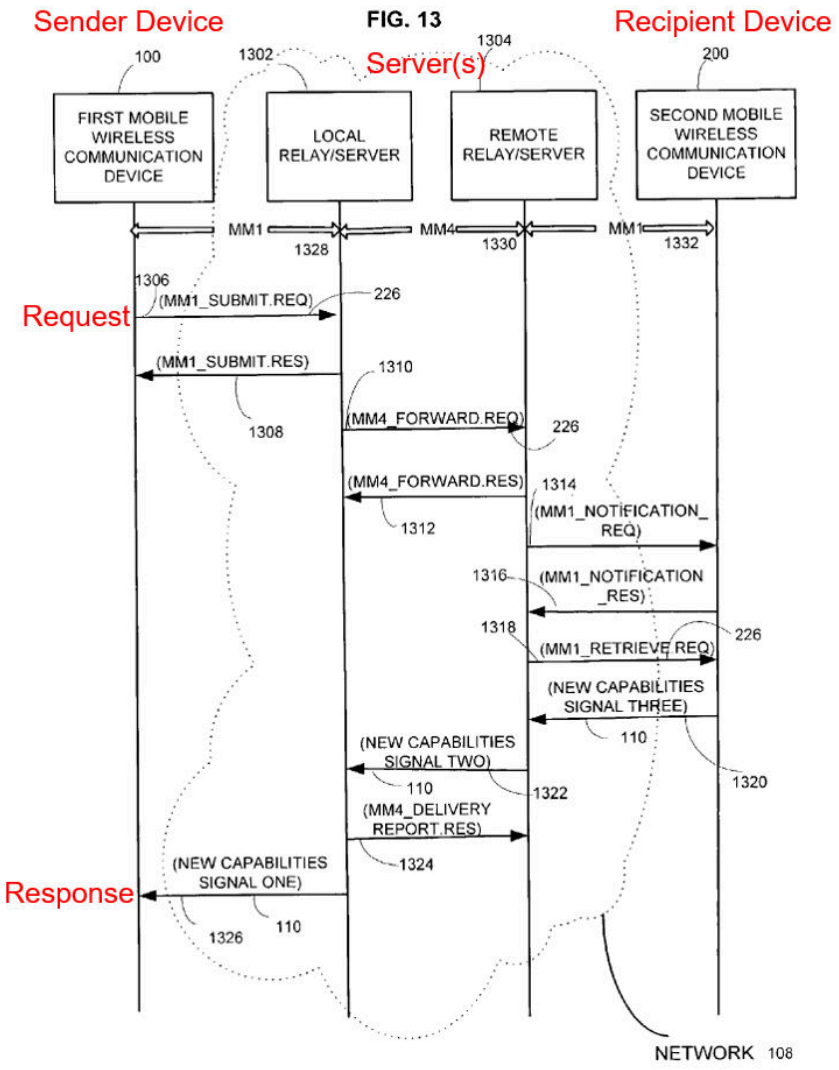
capabilities information **request**" to a remote web server, and "receiv[es] a **response** [*e.g.*, from the web server] to the request where the response contains the second mobile wireless communication device messaging format capabilities information 110." APPLE-1005, [0024], [0027], [0042] (both generation of the request and reception of the response "may be accomplished using the remote messaging format capabilities determinator circuitry 208" or "other suitable circuitry"), [0034], [0056]-[0057] ("request and retrieve the second mobile wireless communication device messaging format capabilities information 110," "a second mobile wireless communication device messaging format request 226," "new capabilities signal one 1326 [including] at least the second mobile wireless communication device messaging format capabilities information 110"), FIGS. 6 (below), 13 (below).

35. In some examples, Tsampalis explains that "the second mobile wireless communication device messaging format capabilities information 110 is stored" in "a network element within the network 108" such as "a web server." *Id.*, [0039], [0057] ("note that some embodiments store the second mobile wireless communication device messaging format capabilities information 110 at the remote relay/server 1304, and for such embodiments, signals 1314, 1316, 1318 and 1320 are not used"). In such cases, the first (sender) device can retrieve the second

(recipient) device's MFCI 110 from a remote server using signaling like that shown in FIG. 13 (below). *Id.*; *see also id.*, [0056]-[0060], FIGS. 13-15.



APPLE-1005, FIG. 6 (Annotated)



APPLE-1005, FIG. 13 (Annotated)

36. Tsampalis further explains that the first (sender) device can store the second (recipient) device's MFCI 110 in a phonebook, and can use the second (recipient) device's MFCI 110 to select a suitable message format and corresponding transmission mode (*e.g.*, an SMS, MMS, or EMS transmission) for sending the message based on the capabilities of the second (recipient) device. APPLE-1005, [0041], [0060]-[0064], FIGS. 5, 16.

C. Combination of Horvath and Tsampalis

37. Like the '127 Patent, Horvath describes selective transmission of wireless messages in different transmission modes, including techniques for transmitting messages over either a packet data network or a circuit services network. APPLE-1001, 2:4-12; APPLE-1004, [0001], [0007], [0024]-[0026], [0050], [0061]-[0062], FIGS. 1, 4, 7; *supra*, §VII.A (Horvath). Horvath is concerned with the circuit services network being "unnecessarily burdened with SMS traffic," and proposes to ameliorate this problem by using a packet data network for the transmission of SMS messages by default whenever the sending and receiving devices are registered with a message delivery service on the packet data network (*e.g.*, registered with an SIP network). *See e.g.*, APPLE-1004, [0004], [0006]-[0009], [0021], [0039] (goal to provide "capacity relief on the circuit services network 104"), [0081] (desire to "provide dynamic optimization of the resources available" and to "optimiz[e] network resources").

38. As described above, Horvath's sender device determines whether to send an outgoing SMS message to a server system (*e.g.*, Information Processing System 108 / SMSC 114) over a packet data network or a circuit switched network based on whether the sender is currently registered with a session initiation protocol ("SIP") network on the packet data network. *Supra*, §VII.A (Horvath); APPLE-1004, [0004], [0074]-[0076], FIG. 6 (below). The server system in turn

determines whether to forward the SMS message to the intended recipient device over a packet data network or a circuit switched network based on whether the recipient is registered on the packet data network. *Id.*

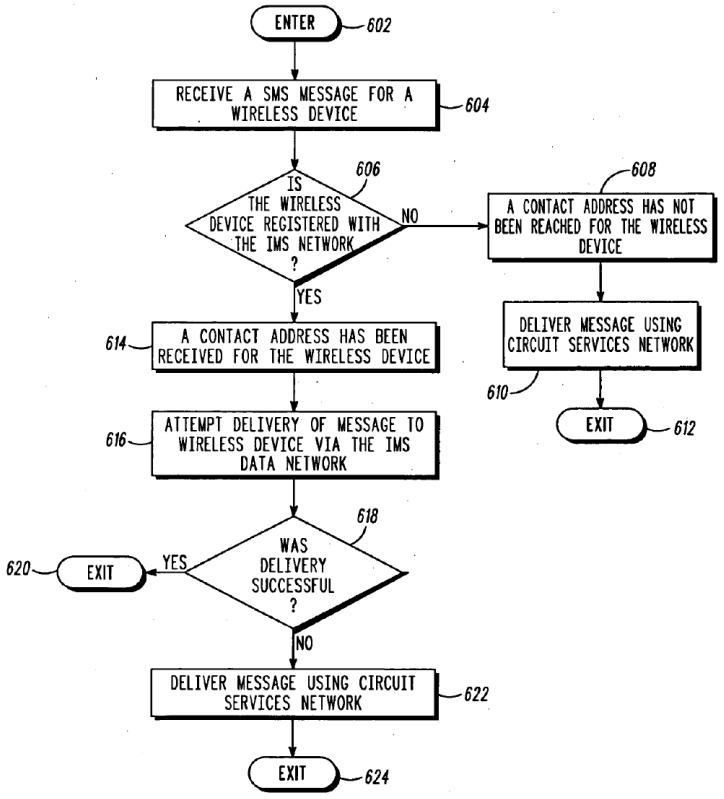


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

39. By diverting SMS messages from the circuit switched network to the packet data network when a device is registered on a packet data network, Horvath's system beneficially reduces load and "unnecessary overhead" on the circuit switched network. APPLE-1004, [0004], [0009]. Notwithstanding these benefits, however, a POSITA would have recognized that Horvath's system was

still ripe for improvement. For example, although Horvath acknowledges additional messaging services apart from SMS (*e.g.*, MMS, EMS, IM), Horvath provides little detail about the additional messaging services. APPLE-1005, [0025], [0039]. Additionally, a POSITA would have appreciated that some users did not necessarily subscribe to each of these messaging services and users often had limited messaging capabilities that precluded them from receiving or processing richer media formats beyond SMS (*e.g.*, MMS, EMS, IM). Consequently, the sender risked sending a message in a format that the recipient would be incapable of processing or presenting to a user. *Id.* This, in turn, resulted in failed message deliveries, re-transmission attempts that further burdened the network, increased processing load on messaging servers, and frustration by users who expected messages to be delivered in one format but which ultimately could not be delivered as expected. APPLE-1005, [0003]-[0004].

40. In view of these known problems with a multi-modal messaging environment like Horvath's in which different mobile device users subscribed to messaging services (*e.g.*, SMS, MMS, EMS, IM), a POSITA would have turned to Tsampalis for specific guidance on how to improve the user experience and better manage and coordinate messaging formats in such an environment. *Supra*, §VII.A (Horvath); §VII.B (Tsampalis). In particular, Tsampalis describes an effective solution for improving messaging in such an environment by sharing the

recipient's messaging format capabilities information with the sender. *Supra*, §VII.B. A POSITA reviewing Horvath and Tsampalis would have found it obvious to implement Horvath's system in accordance with Tsampalis's suggestions for a sender device to obtain and use messaging format capabilities information of a recipient device to determine how to format and transmit an outgoing message to the recipient. Multiple reasons would have prompted a POSITA to combine Horvath's and Tsampalis's teachings in this manner well before the Critical Date of the '127 Patent (July 24, 2007).

41. First, a POSITA would have combined Horvath and Tsampalis such that the sender would obtain and use a recipient's messaging format capabilities information to enhance users' messaging experiences and ensure that the format of outgoing messages is compatible with the messaging format capability of the recipients' device before the message is sent. Tsampalis itself expressly acknowledges the benefits flowing from these techniques, noting that "the determining of the message capabilities of a target mobile wireless communication device before sending a message to such target device[] … can enhance a user's experience by allowing a user to determine whether to attempt to send or modify a message based on the messaging capabilities of the intended recipient(s) of the message" and "by providing the user the ability to select a format in which to send a message based upon the messaging capabilities of the intended recipient(s) of the

message." APPLE-1005, [0065]. Horvath also already considers the challenge of encoding in different network standards, which would further prompt a POSITA to combine with Tsampalis for teachings on formatting compatibility. *See e.g.*, APPLE-1004, [0050] (describing message encoding using "IS-637" versus very different "ANSI-41" standard).

42. Second, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath's system to permit the sender to make more frequent and reliable use of enhanced messaging formats such as MMS and IM. Enhanced messaging formats such as MMS and IM generally offer richer messaging capabilities than SMS, such as the ability to support extended character counts for longer messages and the ability to attach/include multimedia files with the message. APPLE-1007, Page 8 ("IM&P [*i.e.*, Instant Messaging and Presence] service is more media-rich than traditional applications such as mail, phone, and email. By using IM&P, we can deliver voice, video, and data together to various endpoints."); APPLE-1025, Introduction ("The most significant characteristic of MMS is to support multimedia contents. It can send not only texts, but also images, videos and audios. Therefore, MMS applications are much richer than those of SMS."). A POSITA would have understood that the enhanced messaging capabilities of MMS and IM were often desirable for situations where users desired to communicate more than the short,

text-based messages that could be accommodated by SMS. *Id.* If the recipient's messaging capabilities are unknown, however, some senders are biased toward not using any of the enhanced messaging features of MMS or IM to ensure the message is successfully delivered to the recipient using a more basic service (*e.g.*, SMS). *Id.* But intentional avoidance of enhanced messaging features offered by MMS or IM is unnecessary if the recipient is in fact capable of receiving MMS or IM messages, and Tsampalis's proposal to share the recipients' messaging format capabilities information with the sender would allow a sender to use these rich messaging features more frequently and reliably with confidence that the recipient can successfully receive them. *Id.*

43. Third, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath's system to make better, more selective use of SMS when the recipient has limited messaging capabilities. As Tsampalis explains, some users do not subscribe to MMS and are incapable of receiving or processing messages other than SMS or similar text-based messages. APPLE-1005, [0061]-[0063]. By obtaining the recipients' messaging format capabilities information in advance of sending a message, the sender can ensure the message is appropriately sized and formatted according to the restrictions imposed by SMS and the limited messaging capabilities of the recipient. Likewise, the

sender can avoid making use of richer features associated with formats such as MMS or IM that the recipient could not receive or process. *Id.*

44. Fourth, a POSITA would have been motivated to apply Tsampalis's teachings to Horvath in the manner described above to ensure the sender could recognize any incompatibilities between the format of an outgoing message and the messaging format capabilities of the intended recipient of the message *before* the message is sent. In addition to enhancing the user's experience, Tsampalis's approach to making use of messaging format capabilities information before a message is sent would beneficially reduce occurrences of failed message deliveries resulting from attempts to send incompatible message formats. *Id.* It would likewise reduce network traffic and corresponding load on the system by reducing the number of re-transmission attempts stemming from failed message deliveries. APPLE-1005, [0003], [0004] (lamenting prior approaches where "the sending device is unaware of the incompatibility until after the message is bounced back" because "there is no opportunity for the sending device to change the content of the message, change the recipient list associated with the message, or choose not to send the message, before sending a message that will later be bounced back"); [0022]-[0023], [0025].

45. Fifth, a POSITA would have been motivated to apply Tsampalis-like messaging format capabilities information to Horvath's system to advance

Horvath's express objectives of reducing "unnecessary overhead for the system" and "dynamic optimization of [] resources." APPLE-1004, [0004], [0081]. For example, a POSITA would have appreciated that integration of Tsampalis's techniques in the combination would further optimize the sender's determination of a transmission mode (*e.g.*, whether to send an SMS, MMS, or IM, whether to attach any multimedia files, and/or whether to transmit over the packet data network or the circuit services network), while reducing unnecessary burden on the remote server by having the sender device process/format the outgoing message according to the selected transmission mode.

46. Sixth, a POSITA would have naturally looked to Tsampalis, as like Horvath, Tsampalis also teaches various networks for transmitting messages of different formats, including "a cellular wireless network, internet or other suitable network." APPLE-1005, [0028].

47. Seventh, a POSITA would have found it obvious to combine the teachings of Horvath with Tsampalis because the combination merely involves the application of a known technique to a known system to achieve predictable results. Tsampalis recognized a known problem with dynamic messaging environments like Horvath's in which users have different messaging format capabilities, and yet, Tsampalis's teachings would help address this problem in a straightforward manner that was well within the skill of a POSITA. A POSITA would have further

recognized that at the time of the claimed invention, some users were still charged on a per SMS basis, and being selective about how messages were sent could save costs for both the sender and the receiver. APPLE-1009, 1 ("Sending an SMS message to a mobile telephone carries an attached cost for sending the message over the mobile network…A user of a mobile device whilst in a location with WiFi (or other form of) internet access would authenticate with the remote registration server and this would indicate to the Routing System that it was possible for that mobile device to receive text messages via the internet rather than via GSM SMS messages offering substantial cost savings to the sending party. Replies could also be made over the internet providing further costs savings."). Accordingly, the combination would have been obvious.

48. Likewise, a POSITA would have reasonably expected success implementing the combination, especially since the resulting system could be implemented with conventional software and hardware techniques (*e.g.*, general-purpose processors on mobile devices executing programmable instructions) with messaging formats (*e.g.*, SMS, MMS, IM) that were well-defined and commonly implemented by the Critical Date of the '127 Patent. Further, the techniques that would be integrated from Tsampalis in the Horvath-Tsampalis combination are fully compatible with Horvath's and would not disturb the ability of Horvath's system to transmit or deliver SMS messages over either a packet-based on circuit

switched network. Indeed, Horvath and Tsampalis both describe multi-modal wireless devices that are physically and logically compatible with each other. As discussed above, Horvath and Tsampalis are also both analogous art to the '127 Patent, each being in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '127 Patent. For example, like the '127 Patent, Horvath and Tsampalis both describes methods and systems for mobile messaging over wireless networks. *Supra*, §VI.A, §VII.A-B.[3]

49. Finally, a POSITA would have found it obvious to extend Tsampalis's messaging format capabilities information in the combination system to further indicate an intended recipient's instant messaging capability like that described in Horvath (e.g., in addition to SMS, MMS, EMS capabilities), and there would be no incompatibility between Tsampalis's teachings and the addition of instant messaging as an identifiable messaging capability of a device. A POSITA would have understood that identifying additional messaging capabilities of the intended

---

[3] The overview of the Horvath-Tsampalis combination described in §VII.C is incorporated in the analysis of each claim element in §VIII.A below. For claim elements in which this Declaration cites Horvath's teachings alone, it is understood that those teachings are applicable in the combination and are not negated by the combination with Tsampalis.

recipient of a message, including information indicating whether the intended recipient is capable of receiving instant messages, would further Tsampalis's goal of enabling the sending device to select an optimal message format before sending a message, thereby enhancing the user's experience and reducing attempts to transmit a message in a format that the recipient is either incapable of receiving or that does not make best use of the recipients' messaging capabilities. APPLE-1005, [0065], [0003]-[0004]. Tsampalis identifies SMS, MMS, and EMS as "non-real-time store and-forward messaging format capabilities," but Tsampalis does not restrict the messaging format capabilities information from further including other messaging formats. On the contrary, Tsampalis contemplates that any suitable messaging format can be indicated in the messaging format capabilities information. APPLE-1005, [0022] (describing non-real time store-and-forward as a mere example of messaging format capabilities information ("***such as***")), [0025] (explaining that messaging format capabilities information can include "data representing that the device can process messages that are in an SMS format, EMS format, or ***another suitable format***"). A POSITA would have desired to inform the sender of all messaging format capabilities of the recipient, including IM, to provide the sender with comprehensive information that would better allow the sender to optimize its selection of a format for messaging the recipient. *See also* APPLE-1007, 6 (describing known option for "store-and-forward" IM services).

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '127 CLAIMS UNPATENTABLE

A. The Horvath-Tsampalis Combination Renders Claims 1-20 Obvious

Element [1pre]: A method of providing a messaging service for use in a wireless device of a sender, the method comprising:

50. To the extent the preamble is limiting, the Horvath-Tsampalis combination renders obvious [1pre].[4] For example, Horvath discloses services for "transmitting at least one short messaging service message" between two or more "wireless devices." *See e.g.*, APPLE-1004, Abstract ("A method and device for transmitting at least one short messaging service message to at least one wireless device are disclosed."), Title ("METHOD AND SYSTEM FOR DELIVERY OF SHORT MESSAGE SERVICE MESSAGES"), [0002] ("Short message service ('SMS') is a service that allows a wireless device such as a mobile phone to send and receive short messages from other wireless devices."), [0006] ("disclosed are a method and device for transmitting at least one short messaging service message."), FIG. 5 ("wireless device transmits..."). Horvath likewise describes an ability of the sender wireless device to transmit enhanced messaging service ("EMS") messages,

[4] This Declaration incorporates the description of the Horvath-Tsampalis combination from §VII.C into the analysis of each element of the Challenged Claims.

multimedia messaging service ("MMS") messages, instant messages, and the like. APPLE-1004, [0025], [0033].

51. Horvath's FIG. 4 (below) further shows an example "wireless device 106" that communicates on "either the packet data network 102 or the circuit services network 104." APPLE-1004, [0014], [0060]-[0070].

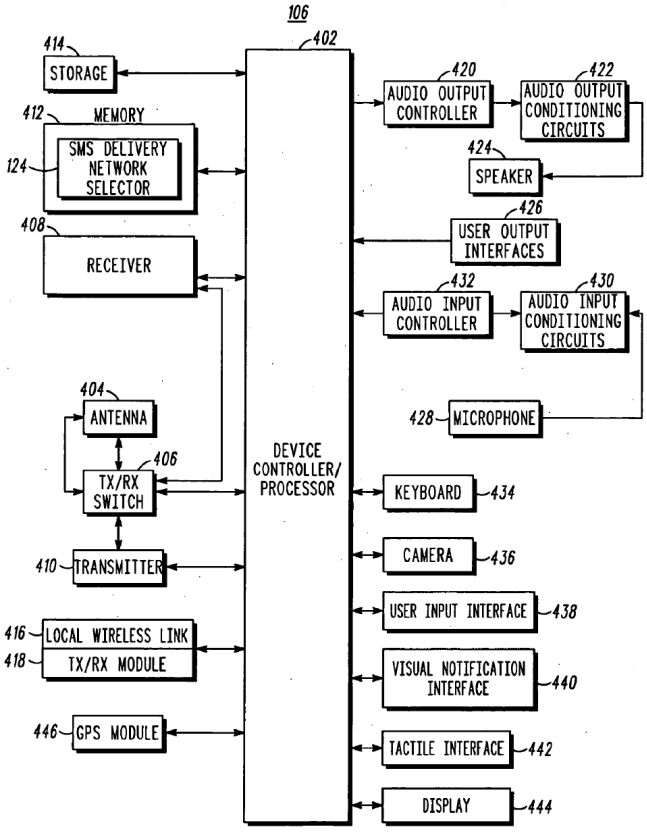


FIG. 4

APPLE-1004, FIG. 4

52. As shown in Horvath's FIG. 7, the sender wireless device "select[s] a network for transmitting a SMS message based on what network the wireless device is registered with." APPLE-1004, [0017], [0078].

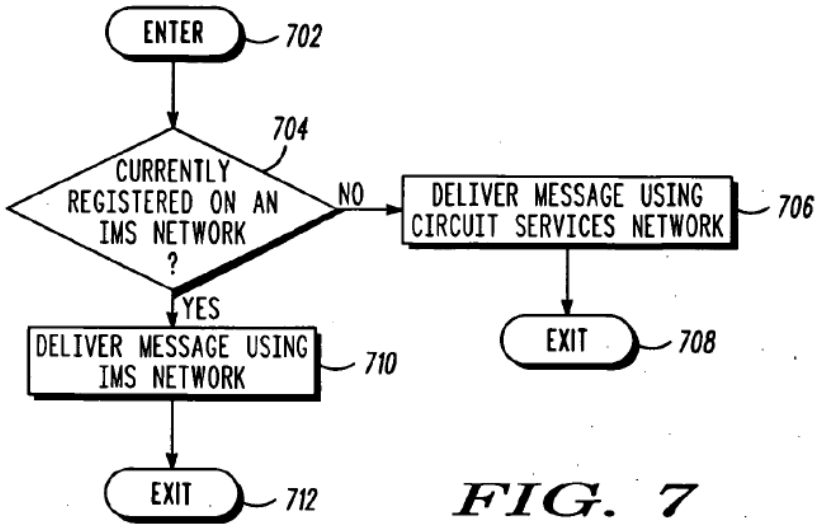


FIG. 7

APPLE-1004, FIG. 7 (Sender Device Perspective)

Element [1a1]: receiving, by a message client running on the wireless device of the sender, information associated with a destination address of a wireless device of a recipient,

53. Horvath-Tsampalis renders obvious [1a1]. For example, Horvath explains that the wireless device, e.g., wireless device 106, sends messages to recipient wireless devices over one or more packet data networks 102 and/or circuit switched networks 104. APPLE-1004, [0050] ("wireless device 106[] … is configured to transmit SMS messages to another device"), [0078], FIG. 7. From Horvath's disclosures in this regard, a POSITA would have understood that the sender wireless device receives information associated with a destination address of a wireless device of the recipient, especially since the intended recipient would need to be addressed in the message to be delivered to the desired recipient device.

54. Horvath further teaches that the recipient can be addressed by a contact address such as a universal resource indicator (URI) formed from a telephone number or other registered information about the recipient. APPLE-1004, [0050] ("the destination address of the recipient device is a SIP URI formed out of the normal address (for example, tel:MDN)"), [0035] ("HSS 210 also includes information to identify each registered wireless device 106 such as a telephone uniform resource identifier ("tel-URI") and/or a SIP uniform resource identifier ("SIP-URI"). A tel-URI, for example is the telephone number assigned to the wireless device 106."), [0043]-[0046], [0073]. Horvath's functionality for receiving information associated with a destination address of a recipient is maintained in the combination with Tsampalis, which similarly describes conventional addressing techniques where the sender receives phone numbers of intended messaging recipients. APPLE-1005, [0061] ("first mobile wireless communication device 100 will transparently contact the network talking to the address(es), (e.g., the MSISDN(s)), of the recipient(s)"), [0033] ("As the active message recipient list 218 is populated with each recipient ID 402…"), [0046], ("Block 1008 demonstrates the method including the receiving of a next recipient ID 402 as the recipient ID is entered in the send message circuitry 106"), [0064] ("the user is composing a test message"), FIGS. 3-4 (showing phone numbers as recipient IDs), 7, 10.

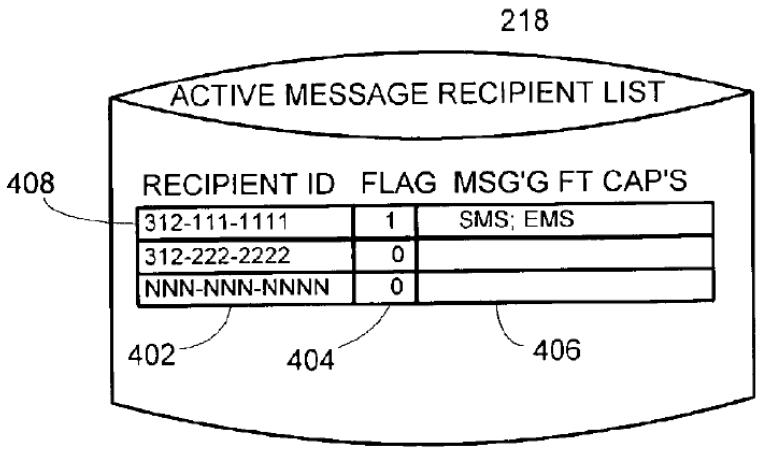


FIG. 4

APPLE-1005, FIG. 4

55. A POSITA also would have understood that the sender device in the Horvath-Tsampalis combination includes a "message client" to receive the phone number or other information associated with a destination address of the recipient. For example, Horvath explicitly discloses that the sender device executes messaging software to carry out messaging functions, much like the '127 Patent, and in the combination this would include functionality for receiving information identifying the intended recipient of a message. APPLE-1004, [0061]-[0062], FIG. 4. A POSITA would have understood such software to provide a "***messaging client***" as claimed. *Id.*; *cf.* APPLE-1001, 5:2-3 ("the invention is a software program to implement the method"), 5:49 ("a message client 114 runs on the mobile device").

56. Providing a message client on the sender device also would have been obvious to ensure the sender device was equipped with suitable software to carry out the messaging functions of the Horvath-Tsampalis combination as described herein. These functions align with the types of functions that were commonly performed by messaging clients before the Critical Date. APPLE-1008, [0038] ("The transmitting terminal (10) is a mobile communication terminal having **an instant message client installed therein**"), [0002] ("The present invention relates to a messaging service for a mobile communications terminal, and in particular, to a system and method for interworking messages of a mobile communications terminal that receives multimedia contents transmitted by using an instant messaging (IM) client."), [0004] ("Message services for mobile communication terminals can be broadly divided into instant message (IM) services, multimedia message services (MMS), and short message services (SMS). As instant message clients are being installed in mobile communication terminals, instant message services based on wired Internet technology are being expanded into the field of mobile communications."); APPLE-1009, page 3 ("The mobile GSM device would have an operating system capable of running **an application** which could subscribe and log into a registration server when the device gained access to the internet via a route such as bluetooth, Wifi (802.11 b,g or other), or via infrared or any other packet radio (eg GPRS) or other electromagnetic means. The mobile device would

register with the remote registration server and this registration would inform the Routing System that the message could be sent via the internet based connection rather than via the GSM network if required. The registration server could be either a dedicated solution using normal web based protocols such as http post or get, or via SIP, SMPP or other protocol which allows authentication with a remote device."), page 6 ("A Routing System utilising [*sic*] of Software capable of being installed and operated on a mobile device which, once authenticated with a remote database, can be sent text messages via IP based protocols such as (but not necessarily via) SIP, XML or HTTP"); APPLE-1017, 34:63-66 ("...Instant Messenger **software** such as is provided by Microsoft, America On Line, AT&T and others. These programs provide notification when a computer-messaging device is on line or the operator is logged in."); APPLE-1021, 4:66-5:6 ("Mobile devices 102-104 may further be configured to include **a client application** that enables the end-user to log into an end-user account that may be managed by another computing device, such as ENS 106. Such end-user account, for example, may be configured to enable the end-user to receive emails, send/receive IM messages, SMS messages, access selected web pages, participate in a social networking 5 event, or the like."), 9:57-64 ("MM [Message Managers] 245 represents any of **a variety of applications** configured to transmit, receive, and/or otherwise process messages and other network content, including, but not limited

to SMS, MMS, IM, email, VOIP, browsers, or the like, and to enable telecommunication with another user of another networked device."), 10:3-50 ("MM 245 may further include **an IM application** that is configured to initiate and otherwise manage an instant messaging session, including, but not limited to AOL Instant Messenger, Yahoo! Messenger, NET Messenger Server, ICQ, and the like. In one embodiment, the IM application within MM 245 may be configured to employ a SIP/RTP to integrate IMNOIP features. For example, the IM application may employ SIMPLE (SIP for Instant Messaging and Presence Leverage), APEX (Application Exchange), Prim (Presence and Instant Messaging Protocol), Open XML-based XMPP (Extensible Messaging and Presence Protocol), more commonly known as Jabber and OMA (Open Mobile Alliance)'s IMPS (Instant Messaging and Presence Service) created specifically for mobile devices, or the like."); *see also* APPLE-1005, [0024] (Tsampalis describing its circuitries on a sender wireless device for determining recipient messaging capabilities and for sending messages as "software modules"), [0027], [0046], FIGS. 3-4, 7, 10.

Element [1a2]: the message client capable of determining a transmission mode for sending an outgoing message to the wireless device of the recipient,

Element [1a3]: wherein the wireless device of the sender is capable of sending messages in a plurality of transmission modes comprising a first transmission mode and a second transmission mode;

57. Horvath-Tsampalis renders obvious [1a2]-[1a3]. As discussed above, the sender device in the Horvath-Tsampalis combination determines parameters for transmitting a message to a recipient device based on factors including the sender device's current registration status with a packet data network 102 and information about the messaging format capabilities of the intended recipient. *Supra*, §VII.C. For example, the sender device determines whether to send an outgoing message as an SMS, MMS, or IM message based on the recipient's messaging format capabilities information, as taught in Tsampalis, and the sender device further determines whether to transmit an SMS message over the packet data network 102 or circuit services network 104 based on whether the sender device is currently registered with the packet data network 102, as taught in Horvath. *Id.*; APPLE-1004, Abstract, [0004], [0006]-[0009], [0024]-[0026], [0028], [0033]-[0039], [0045], [0050], [0061]-[0063], [0074]-[0076], [0078], [0080]-[0081], FIGS. 1-4, 6-8; APPLE-1005, Abstract, [0004], [0022], [0024], [0027], [0033]-[0035], [0039], [0041]-[0042], [0045], [0056]-[0057], [0060]-[0065], FIGS. 2, 5, 6, 9, 13.

58. Again, Horvath discloses that the sender device determines a transmission network and corresponding protocol for sending an SMS message to the recipient device based on whether the device is currently registered with a packet data network. APPLE-1004, [0050], [0062], [0078], FIGS. 1, 4, 7 (below); *supra*, §VII.C, §VIII.A, Analysis of Element [1a1].

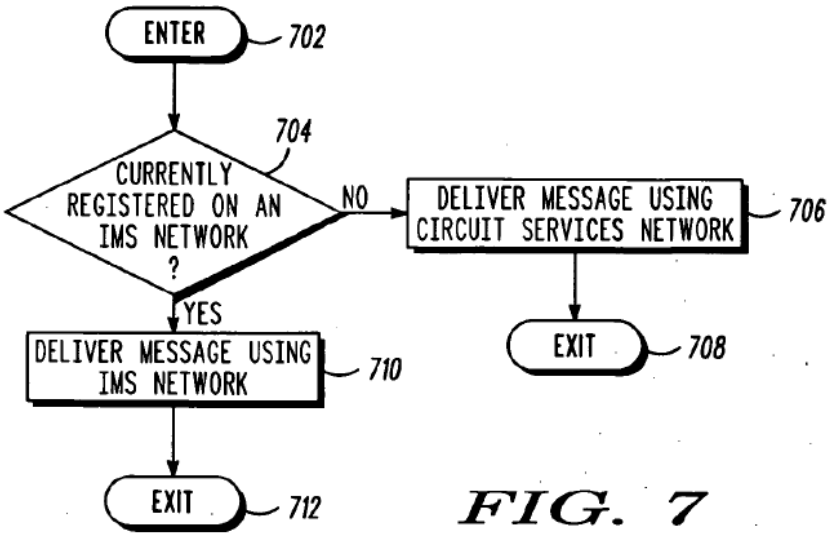


FIG. 7

APPLE-1004, FIG. 7 (Sender Device Perspective)

59. Further, as discussed above, based on Tsampalis, it would have been obvious for the sender device to optimize the format and hence transmission mode of an outgoing message based on information about the recipient's messaging format capabilities. *Supra*, §VII.C; APPLE-1004, [0004], [0081]; APPLE-1005, [0065]. For example, the sender device can obtain information about the recipient device's messaging format capabilities before sending a message, in accordance with Tsampalis, further advancing Horvath's express objectives of reducing "unnecessary overhead for the system" and "optimizing network resources," while also "enhanc[ing] a user's experience" as taught in Tsampalis. *Id.* A POSITA would have understood, and it would have been obvious, that a messaging client on the sender device would provide the device's messaging capabilities, including

capabilities for determining a transmission mode, for the reasons discussed above with respect to [1a1]. *Supra*, Analysis of Element [1a1].

60. In combination, the plurality of transmission modes that the Horvath-Tsampalis sender device is capable of sending would predictably include (i) an **MMS-based transmission mode** that involves sending an MMS formatted message over the packet data network 102, (ii) an **IM-based transmission mode** that involves sending an instant message over the packet data network 102, and (iii) an **SMS-based transmission mode** that involves sending an SMS formatted message over the packet data network 102 or circuit services network 104. APPLE-1004, [0025], [0033] ("instant messaging" being "real-time"), [0039] (describing IM, MMS, and SMS messaging services); APPLE-1005, [0002] (describing SMS, EMS, MMS and the "non-real-time store-and -forward" characteristic), [0024], FIG. 1 (disclosing MMS and SMS messaging services); *supra*, §VII.C, §VIII.A, Analysis of Element [1a2]; APPLE-1007, 1 ("Instant messaging (IM) …enables [message] exchanges in real time independent of locale"); APPLE-1010, Abstract, 2:53-63, 5:55-8:50 (identifying SMS, MMS, and IM as different "communication modes"), 9:46-48). The MMS- and IM-based transmission modes each provides (in the alternative) a "***first transmission mode***" as claimed while the SMS-based transmission mode provides a "***second transmission mode***" as claimed.

61. More specifically, Tsampalis discloses that the sender can set a "default format" for outgoing messages from the sender device, and the sender device will format a message according to the "default format" so long as the recipient is capable of receiving messages in the default format (otherwise the sender will select a non-default format within the recipient's messaging format capabilities). APPLE-1005, [0062] ("[A] message may be initially formatted in the default messaging capabilities of the sending device, (e.g., MMS format), and if necessary, may be reformatted in a new format, (e.g., SMS), before being sent."), [0036]-[0037], [0048]-[0054], [0062], [0064], FIG. 11. Tsampalis teaches that a rich media format such as MMS is desirable to set as the default format, thereby allowing the sender to access the enhanced features of such a format, including longer messages and optional multimedia attachments, by default. *Id.*, [0062], [0064]. Based on Tsampalis's teachings in this regard, it would have been obvious for the sender device in the Horvath-Tsampalis combination to set MMS or IM as the default messaging format to leverage the enhanced capabilities of those formats over SMS. The sender device would then send MMS or IM messages by default when the sender is connected to the packet data network 102 and the recipient's messaging format capabilities indicate that the recipient is capable of receiving MMS or IM messages. The sender would send SMS messages when the sender is not connected to the packet data network 102 or the recipient's messaging format

capabilities indicate that the recipient is incapable of receiving MMS or IM messages (i.e., the recipient has limited messaging capabilities). If the recipient has limited messaging capabilities such that it cannot receive MMS or IM messages, the sender would determine whether to send the SMS message over packet data network 102 or circuit services network 104 based on whether the sender is currently registered on the packet data network 102 as taught in Horvath. APPLE-1004, [0050], [0078], FIG. 7.

62. A POSITA further would have understood that MMS, IM, and SMS represent not just different message *formats* but also different *transmission modes* due to fundamental differences in how MMS, IM, and SMS messages are transmitted from a sending device, processed by the network, and delivered to the recipient. For example, MMS and IM are much richer than text-only SMS, and they each employ different transmission protocols. APPLE-1004, [0033] ("instant messaging" being "real-time"); APPLE-1005, [0002] (describing SMS, EMS, MMS and the "non-real-time store-and -forward" characteristic); APPLE-1007, 1 ("Instant messaging (IM)…enables [message] exchanges in real time independent of locale"), 8 ("IM&P service is more media-rich than traditional applications such as mail, phone, and email. By using IM&P, we can deliver voice, video, and data together to various endpoints."); APPLE-1025, 1-2 ("MMS applications are much richer than those of SMS. MMS supports JPEG and GIF image

formats…Attractive MMS applications are based on advanced technologies. First, MMS is supported by the Wireless Application Protocol (WAP)…. MMS is based on the General Packet Radio Service (GPRS). GPRS is an efficient way of data transmission based on packet switch…As a 3G service, the MMS will be a key mobile value-added service."); APPLE-1036, page 2, line 25 -page 4, line 25 ("The Short Message Service - Point to Point (SMS-PP) is defined in GSM recommendation 03.40. GSM 03.41 defines the Short Message Service - Cell Broadcast (SMS-CB) which allows messages (advertising, public information, etc.) to be broadcast to mobile users in a specified geographical area. Messages are sent via a store-and-forward mechanism…Transmission of the short messages between SMSC and phone can be done through different protocols such as SS7 within the standard GSM MAP framework or TCP /IP within the same standard. Messages are sent with the additional MAP operation forward short message, whose payload length is limited by the constraints of the signaling protocol to precisely 140 bytes (140 bytes = 140 * 8 bits = 1120 bits)...Multimedia Messaging Service (MMS) is a standard for a telephony messaging systems [*sic*] that allow sending messages that includes multimedia objects (images, audio, video, rich text) and not just text messages as in Short message service (SMS)…. MMS is the evolution of Short Message Service (SMS)…MMS has been designed to work with mobile packet data services such as GPRS and lx.").

63. Brugge (APPLE-1042) further describes a range of differences between the protocols for MMS, SMS, and instant messaging that a POSITA would have understood to distinguish them as different transmission modes. For example, Brugge explains that the size of an MMS message is capped at 100 kBytes while an SMS message is limited to 140 bytes or 160 characters. APPLE-1042, 5. Brugge also explains that "[a]ll elements of an MM are included within a single SMTP 'mail' message, which is organized as MIME (Multipurpose Internet Mail Extensions) encoded message with the appropriate 'Content-Type' [44] header field value …. All MM elements are of standard MIME content types." APPLE-1042, 11. An SMS message, by contrast, comprises text with no ability to freely add images or voice attachments. APPLE-1042, 5. The sending device must therefore apply different protocols, different character types, and different constraints when formatting and preparing SMS vs. MMS messages for transmission. *See generally* APPLE-1042. I've noted that Patent Owner's infringement contentions likewise identify "SMS" as a "second transmission mode" and identify a different messaging service (iMessage) as a "first transmission mode." APPLE-1101, 16-20.

Element [1b1]: determining, by the wireless device of the sender, whether the destination address corresponds to a subscriber of a service for receiving the outgoing message via a packet switched bearer

Element [1b2]: by sending a request via a packet switched wireless local area network (WLAN) base station to a server,

Element [1b3]: and receiving a response from the server via the packet switched WLAN base station, the response providing an indication of whether the destination address corresponds to a subscriber of the service;

64. Horvath-Tsampalis renders obvious [1b1]-[1b3]. As further described below, the sender device in the Horvath-Tsampalis combination determines whether the destination address corresponds to a subscriber of a service for receiving the outgoing message via a packet switched bearer in at least three ways:

Option (1): determining from messaging format capabilities information whether the recipient is capable of receiving/processing MMS messages;

Option (2): determining from messaging format capabilities information whether the recipient is capable of receiving/processing IM messages, and

Option (3): determining from registration or presence information whether the recipient is currently available on a packet-based SMS or IM service.

Supra, §VII.C, §VIII.A, Analysis of Element [1a1]. Each of these three techniques independently renders obvious [1b1]-[1b3]. *Id.*

65. In more detail regarding **option (1)**, Horvath discloses MMS as a messaging service for communicating messages from a sender to a recipient device. APPLE-1004, [0025], [0039]. Tsampalis similarly discloses MMS as a desirable messaging service. APPLE-1005, [0002]-[0003], [0024]. By the relatively late Critical Date of the '127 Patent, a POSITA would have been familiar with MMS and would have recognized it as a packet-based service that uses a packet switched

bearer to deliver MMS messages to recipient devices. *See, e.g.*, APPLE-1025, 1-2 ("MMS applications are much richer than those of SMS…. MMS is based on the General Packet Radio Service (GPRS). GPRS is an efficient way of data transmission based on packet switch…As a 3G service, the MMS will be a key mobile value-added service."); APPLE-1036, page 2, line 25 - page 4, line 25 ("Multimedia Messaging Service (MMS) is a standard for a telephony messaging systems [*sic*] that allow sending messages that includes multimedia objects (images, audio, video, rich text) and not just text messages as in Short message service (SMS)….MMS has been designed to work with mobile packet data services such as GPRS and lx."); APPLE-1042, . That is, unlike SMS, MMS messages were generally not capable of being delivered by a circuit-switched bearer, especially by the Critical Date of the '127 Patent (July 24, 2007) when packet-switched bearers like GPRS predominated and operators typically would not support circuit-switched bearers for multimedia message transport. *See* APPLE-1042, 7 ("MMS is based on the wireless application protocol (WAP), which runs over either: packet switched data (GRPS/3GPP)"), *id.*, ("today GRPS is mostly used"), *id.*, ("The mobile [] activates a GRPS context and receives the MMS."). MMS instead exploits the unique features and additional bandwidth offered by packet switched networks to permit transmission of longer and more feature-rich messages than SMS. With this knowledge, a POSITA would have

understood MMS to be a service for receiving an outgoing message via a packet switched bearer.

66. Paragraph [0025] of Horvath discloses that "[t]ext messaging standards such as Short Message Service ("SMS"), Enhanced Messaging Service ("EMS"), Multimedia Messaging Service ("MMS"), and the like are also included in the networks 102, 104. APPLE-1005, [0025]. A POSITA would have understood this disclosure to mean that different ones of the messaging standards can be included in one of the networks 102, 104 that ordinarily support the respective standards. As explained above, operators did not ordinarily support MMS on a circuit services network, and MMS was predominantly implemented on packet switched networks. Even if, in an uncommon instance, MMS were ever supported on a circuit services network, it does not detract from the fact that MMS is a service for receiving messages via a packet switched bearer (e.g., GPRS). Nothing in the plain language of the claim requires that the service never be capable of communicating messages via a circuit-switched bearer. Thus, determining whether the destination address corresponds to a subscriber for receiving an outgoing message via MMS (or IM, as explained below) is tantamount to determining whether the whether the destination address corresponds to a subscriber of a service for receiving the outgoing message via a packet switched bearer.

67. Moreover, because a device would subscribe to an MMS service to receive MMS messages, the sender device in the Horvath-Tsampalis combination would determine whether the destination address (*e.g.*, contact address or phone number) of the intended recipient of an outgoing message is a subscriber of an MMS service (*i.e.*, ***a [first] service for receiving the outgoing message via a packet switched bearer***) by checking whether MMS is an available message format for the intended recipient as indicated by the recipient's messaging format capabilities information, based on Tsampalis's teachings. APPLE-1005, [0022]-[0025], [0041], [0056]-[0065], FIGS. 5-6, 13; APPLE-1004, [0038] ("the services subscribed to by the device 106 can be provided"); *supra*, §VII.B-C; APPLE-1025, 3 ("MMS subscriber database"); APPLE-1036, page 3, line 25-26 ("MMS data flow starts with a subscriber using an MMS client on the mobile phone to compose, address, and send an MMS message to one or more recipients."), page 4, lines 1-25. Indeed, a POSITA would have understood that a recipient device would not be capable of receiving and processing an MMS message (such that it would be identified as an available messaging format in Tsampalis's messaging format capabilities information) unless the device corresponded to a subscriber of an MMS service. A subscription to an MMS service was always, or nearly always, required for an intended recipient to be capable of receiving an MMS message sent from another user's device. *See, e.g.*, APPLE-1040, [0009] ("These conditions

and … are not limited to ***MMS messaging***. By contrast the foregoing conditions … may similarly apply to other types of messaging or similar non-connection-oriented services that likewise ***require*** ***that the intended recipient have certain subscriptions*** and/or settings in order to participate in a session of that service (e.g., email, ***instant messaging*** and/or download services).”), [0005] (describing condition requiring that “the intended recipient has a ***subscription*** for the data bearer …, as well as for the ***MMS***”), [0003] (“The MMS client may comprise an individual possessing an ***MMS subscription***”)APPLE-1041, 2-3 (distinguishing “mobile penetration” generally from users having an “MMS subscription” specifically); APPLE-1038, [0072] (“the first terminal sends a request for ***subscribing to an MMS service***”), [0074] (“To validate the ***subscribed MMS service***, the ***subscription to the MMS service*** needs to be activated in this step.”), [0100] (“the ***subscribed MMS service*** is activated”); APPLE-1039, [0057] (“The network operator may chose to use various data elements in order to selectively redirect registration traffic. For example, pre-paid users may need to be redirected to a specific network while post-paid users are be redirected to another preferred network in the same country and coverage area. Even within these segments, the operator may have business rules to determine if the roamer is a GPRS/***MMS subscriber*** or just a voice call user. Based on such service profile information, further preference for networks can be established. Some of the database entities

that are envisaged by this patent application are listed below."), [0063] ("A Subscription Identification databases includes information regarding pre-paid, post-paid, GPRS, and ***MMS subscribers***. Pre-paid roamers are typically identified using a database that is populated by the operator. Similarly, the database has information on GPRS and MMS subscription. The ISD messages on the roaming links can be monitored to identify pre-paid roamers (for example, using CAMEL service mark and SCF address).").

68. Moreover, to be clear, a POSITA would have understood the indications of supported messaging formats in Tsampalis's messaging format capabilities information to represent not only a device's physical capabilities or potential to receive messages of a particular format (e.g., SMS, EMS, MMS, IM), but also whether the device actually has a subscription to the respective messaging services for the formats identified in its capabilities information such that the device would be capable of utilizing those services as needed to receive the messages. This is evident from Tsampalis's explanation that "messaging format capabilities information 110 may be data representing that the device can ***process*** messages." APPLE-1005, [0025]; *see also id.*, [0022] ("send a message … in a format that can be ***processed*** by the target mobile wireless communication device"). Tsampalis sought to reduce failed message delivery attempts by providing senders with the target device's messaging capabilities information so that senders would

be less likely to attempt transmission of messages in formats that could not actually be delivered to the recipient. APPLE-1005, [0065], [0002]-[0004], [0022]-[0023]. If the capabilities information was based only on the physical capability of the device without account for whether the device was subscribed to the corresponding messaging services, Tsampalis would not have achieved the goals it proclaims to achieve. For example, this would have left the recipient of the capabilities information with a misleading indication that a target device was capable of receiving a message in a particular format, even if messages in that format could never actually be delivered to or processed by the target device due to the target device's lack of subscription to a service (e.g., an MMS subscription). This is inconsistent with Tsampalis's disclosure and not how a POSITA would have understood Tsampalis's descriptions of capabilities information or the problems and solutions described therein. In short, a POSITA would have understood Tsampalis's messaging format capabilities information to indicate the capabilities of the target device to ultimately receive and process messages of different types/formats, which is itself indicative of whether the target device corresponds to a subscriber of each of the different messaging services for different message formats (e.g., SMS, MMS, EMS, IM).

69. In the combination, Tsampalis further confirms that it would have been obvious for the sender to determine whether the destination address

corresponds to a subscriber of an MMS service by sending a request to a remote server and receiving a response from the server indicating the same. *Supra*, §VII.C. For example, based on Tsampalis's express teachings, the sender device in the Horvath-Tsampalis combination would send a request to a remote server for the recipient's messaging format capabilities information and would receive a response that indicates whether the recipient indicated by the destination address (*e.g.*, phone number) is capable of receiving/processing MMS messages—and thus whether the recipient is a subscriber of an MMS service. *Id.*; APPLE-1005, [0022]-[0025], [0041], [0056]-[0065], FIGS. 5-6, 13; *supra*, §VII.B-C.

70. A POSITA also would have understood and found obvious that the sender's request to the server and the response received from the server in the Horvath-Tsampalis combination would be communicated "***via a packet switched wireless local area network (WLAN) base station***" as recited in [1b2]-[1b3]. APPLE-1004, [0021], [0024], [0029], [0033]-[0034], [0050], [0081], FIG. 1. For example, Horvath teaches that the sender device transmits messages over a packet data network 102 by default to unburden the traditional circuit services network 104. *Id.* Horvath explains that "packet data network 102 is an Internet Protocol ('IP') connectivity network, which provides data connections at much higher transfer rates then [*sic*] a traditional circuit services network," and comprises "an 802.11 network," which is commonly known as Wi-Fi (a WLAN that operates

based on the IEEE 802.11 standards). APPLE-1004, [0021] (the circuit services network is selected only "[i]f delivery…is not possible on the packet data network"), [0024], [0050], [0078], FIG. 7; APPLE-1011, 5:1-33 ("WLAN capabilities including...technology version (such as 802.11[] …)"), 6:27-32 ("WLAN 802 protocols…IEEE 802 networks"), FIG. 5B; APPLE-1009, 1 ("New generation mobile phones in addition to GSM capability also have the ability to access the internet via 802.11 g, b and other related wireless protocols."), 3 ("The mobile GSM device would have an operating system capable of running an application which could subscribe and log into a registration server when the device gained access to the internet via a route such as bluetooth, Wifi (802.11 b,g or other)…"), 4 ("Wi-Fi is an abbreviation for wireless fidelity and is used to refer generically to any type of wireless network based on the IEEE 802.11 standard or similar form of IP based wireless communication"); APPLE-1037 ("When did Wi-Fi become popular? … 2004: The first Wi-Fi-certified devices (cell phones, PDAs and TVs) hit the market."); *see also* APPLE-1004, [0033]-[0034] ("The wireless device 106 can connect to the IMS network using different methods, which all use standard IP.").

71. A POSITA also would have known that IEEE 802.11 WLAN networks are comprised of base stations (also referred to as "access points") that communicate wirelessly with other 802.11 wireless devices (e.g., STAs), and it

therefore would been understood and obvious to a POSITA that the Horvath-Tsampalis sender device (*e.g.*, wireless device 106) would transmit the request to the server and receive the response from the server containing the recipient's messaging format capabilities information via a WLAN base station. APPLE-1014, [0008] ("a client of the handset detects a signal of a WLAN access point…the trigger is the handset making contact with the access point, which triggers the access point to initiate the registration procedure with the SIP VoIP network"), [0011], [0048] ("a client of the handset detects a signal of a WLAN access point. Once detected by the handset, the handset SIP (session initiation protocol) client initiates a registration procedure over a broadband connection with a WLAN VoIP service located at an application service provider (ASP)"); APPLE-1015, [0027] ("Base station 120, including its associated controller and antenna tower 118, provides wireless network coverage for a particular coverage area commonly referred to as a 'cell'.").

72. As discussed above, Horvath aims to unburden the traditional circuit service network by transmitting messages over the packet data network whenever possible. APPLE-1004, [0004], [0009] ("An advantage … is that the transmission of SMS messages can be done on a packet data network as compared to a circuit services network. If delivery of the SMS message is not possible on the packet data network, the system of the present invention is able to select the circuit services

network for SMS delivery. … A further advantage of the present invention is that a wireless device is able to select either a packet data network or a circuit services network to transmit a SMS message depending on what type of network it is currently registered with."). Accordingly, a POSITA would have understood and found obvious that when Horvath-Tsampalis's sender device is registered with the IMS packet data network which comprises "an 802.11 network" (WLAN), the request that the sender device sends to the server and the response to the request back from the server are both transmitted via the packet switched WLAN base station (*e.g.*, Wi-Fi router) between the sender device and the remote server. APPLE-1004, [0004], [0009], [0024], [0029], [0033]-[0034], [0081], FIG. 1.

73. Regarding **option (2)**, Horvath discloses IM as another messaging service for conveying messages from a sender to a recipient device. APPLE-1004, [0033]. Horvath describes "instant messaging" as a "real-time communications" service that is established using "[t]he SIP network." *Id.* A POSITA would have been familiar with IM services like those described in Horvath before the Critical Date of the '127 Patent, including IM services established using SIP. APPLE-1007 (2005 publication providing an overview of "Instant Messaging and Presence Technologies" and various standards), page 4 ("Instant messaging (IM)…enables [message] exchanges in real time independent of locale…Popular IM applications include AOL™ Instant Messenger (AIM), ICQ™ ("I Seek You"), MSN™ or

WindowsXP™ Messenger, and Yahoo™ Messenger."), Table 1. Consistent with Horvath's explanation that the SIP network is implemented on a packet data network 102, a POSITA would have recognized IM as a packet-based service that uses a packet switched bearer to deliver IM messages to recipient devices. APPLE-1004, [0024] ("In one embodiment, the packet data network 102 is an **Internet Protocol ('IP') connectivity network**, which provides data connections at much higher transfer rates then [*sic*] a traditional circuit services network."), [0033]-[0034], [0037] (messages are sent over the SIP network in "**SIP packets**"); APPLE-1005, [0002], [0022], [0024]; APPLE-1007, page 7 ("the network packet with message Hello! sent from Alice@foobar.com to Bob@foobar.com is represented in Box 1. The **network packet** was captured on the source machine (Alice's machine) using Ethereal Network Protocol Analyzer available at http://www.ethereal.com. The packet is not an exact illustration of all the details. It just gives an overview of how the information is stored and transferred on the network…."), Boxes 1 & 2. That is, like MMS but unlike SMS, IM messages are not ordinarily delivered by a circuit switched bearer. A POSITA thus would have understood IM to be a service for receiving an outgoing message via a packet switched bearer.[5] And because a device must subscribe to an IM service like that

[5] Even if other uncommon protocols support instant messaging via a circuit-

described in Horvath to receive IM messages, a POSITA would have understood and found obvious that the sender device in the Horvath-Tsampalis combination would determine whether the destination address (*e.g.*, contact address or phone number) of the intended recipient of an outgoing message is a subscriber of an IM service (*i.e.*, ***a [second] service for receiving the outgoing message via a packet switched bearer***) when it determines whether IM is an available message format for the intended recipient as indicated by the recipient's messaging format capabilities information, based on Tsampalis's teachings. APPLE-1005, [0022]-[0025], [0041], [0056]-[0065], FIGS. 5-6, 13; APPLE-1004, [0038] ("services

---

switched bearer, that would does not detract from the fact that IM is predominantly a service for receiving messages via a packet switched bearer. In fact, Horvath explicitly discloses that its IM sessions are established over SIP, on the packet data network 102 (i.e., a packet-switched bearer). APPLE-1004, [0033]. Nothing in the plain language of the claim requires that the service never be capable of communicating messages via a circuit-switched bearer. Thus, determining whether the destination address corresponds to a subscriber for receiving an outgoing message via a Horvath-like IM service is tantamount to determining whether the whether the destination address corresponds to a subscriber of a service for receiving the outgoing message via a packet switched bearer.

subscribed to by the device 106"); APPLE-1007, page 5 (providing IM subscription examples that "[b]y January 1997, ICQ had 27,000 users with a growth rate of 100 percent per week. Meanwhile, America Online's (AOL) Instant Messenger (AIM) increased its subscribers to ten million users"); *supra*, §VII.C. To this point, Horvath explains that each wireless device must register with the IMS to access services over SIP, and that each registered device has a profile including "subscription related information" maintained in a database by a registrar for the IMS (e.g., home subscriber server 210). APPLE-1004, [0035], [0036] ("The wireless device 106 is assigned to a specific P-CSCF 206 for the duration of the device's subscription to the IMS network."). Horvath also explains that "[t]he SIP network is used for establishing instant messaging" and that the IMS system "includes application servers that host and execute services for the wireless device 106." APPLE-1004, [0033], [0039] ("A service for example, is SMS, MMS, … and the like."). A POSITA would have understood from Horvath's disclosure and knowledge of IMS/SIP that instant messaging is one of the services of the IMS system supported by SIP such that devices capable of establishing instant messaging sessions would need to have subscription information in the IMS system and would have subscribed to an instant messaging service (e.g., an IM service hosted by application server(s)). APPLE-1004, [0033]; APPLE-1043, [0003] (S-CSCF "provides services to the user that the user is subscribed to"),

[0027] (describing details of "a user (IMS) subscription"), [0029] ("Within the IMS service network, application servers (Ass) are provided for implementing IMS service functionality."), [0034] ("an application server must store ... a service configuration for each IMPU" of subscribed users), [0093], FIG. 2. Chatterjee provides additional details about known instant messaging services including services like SIMPLE implemented using SIP and Jabber/SMPP services that all involve subscriptions to the IM service. APPLE-1007, 5 (AIM "increased its subscribers to ten million users"), 8 ("A contact in the roster item indicates that the user has subscribed"), 8 ("subscribed, …, unsubscribed" presence statuses). In short, a POSITA would have understood or at least found obvious that device that is capable of receiving and processing instant messages would be a subscriber to an IM service because users of IM services must ordinarily subscribe to those services. Accordingly, determining whether a target device's messaging format capabilities information includes IM would is tantamount to determining whether the device corresponds to a subscriber of an IM service (i.e., a service for receiving an outgoing message on a packet-switched bearer). In the combination, it would have been obvious based on Tsampalis for the sender to determine whether the destination address corresponds to a subscriber of an IM service by communicating a request/response to/from a remote server for the recipient's messaging format

capabilities information via a packet switched WLAN base station for reasons similar to those discussed above with respect to the MMS option.

74. Regarding **option (3)**, a POSITA would have found it obvious to configure the sender device in the Horvath-Tsampalis combination to determine whether the destination address of the intended recipient of an outgoing message corresponds to a subscriber of an IM service (*i.e.*, ***a [second] service for receiving the outgoing message via a packet switched bearer***) by checking whether the recipient is currently registered with or present on a SIP network that implements the IM service. For example, Horvath teaches that wireless devices can register with a SIP network when they are connected to the packet data network 102 to notify other devices when they are available to receive messages via a packet switched bearer. APPLE-1004, [0006]-[0009], [0021], [0031], [0050], FIGS. 6-7.

75. Although Horvath describes examples that focus on SMSC 114 receiving information about the recipient's current registration status, it would have been obvious for the sender device also to request and receive from a remote server (*e.g.*, HSS 210 or SMSC 114) the recipient's current registration status with the SIP network. APPLE-1044 (a 2004 RFC already establishing the availability of presence functionality for SIP), Abstract ("This document describes the usage of the Session Initiation Protocol (SIP) for subscriptions and notifications of presence"). *Infra*, Analysis of Claims [10], [20]. Indeed, by the Critical Date of

the ’127 Patent, it was well known how to implement an IM client that polled a server for the current registration status (*e.g.*, presence information) of another IM client, and a POSITA would have possessed motivation to poll a server for such information before sending an IM to ensure the recipient was available to receive the message and participate in a real-time IM session. APPLE-1007, 5 (“Watchers can be *fetchers* or *subscribers*. Fetchers pull the value of presence information for a specific *presentity* from the presence service. If a fetcher is fetching information on a regular basis, it is called a *poller*.”). Tsampalis’s teaching to provide the recipient’s messaging capabilities information to the sender also underscores the obviousness of allowing the sender to poll the server for the recipient’s current registration/presence status because it shows how the sender can use information about the recipient to more effectively tailor messaging strategies to the recipient.

76. While messaging format capabilities information would be sufficient by itself for the sender to determine that the recipient is a subscriber to an IM service, real-time registration/presence information would be beneficial to further inform the sender whether the recipient was currently available to receive an IM. An indication based on real-time registration/presence information that the recipient is currently available to receive an IM would also suffice itself to determine that the recipient is a subscriber to the IM service since only subscribers would be present on the SIP network implementing an IM service. For the reasons

explained above, and because IM presence services were conventionally implemented on packet data networks (including an SIP network), it also would have been obvious for the sender wireless device's request for real-time registration/presence information of the recipient, and the corresponding response, to be communicated via a packet switched WLAN base station. APPLE-1004, [0033]; APPLE-1007, 8 (identifying "subscribed" and "unsubscribed" as known presence statuses) .

Element [1c1]: selecting, by the wireless device of the sender, a transmission mode from the plurality of transmission modes,

77. Horvath-Tsampalis renders obvious [1c1]. As discussed above in connection with elements [1a2]-[1a3], in the combined system of Horvath-Tsampalis, the wireless device of the sender is configured to send messages in a plurality of transmission modes including an MMS-based transmission mode, an IM-based transmission mode, and an SMS-based transmission mode, and the message client (*e.g.*, a messaging service application) running on the wireless device of the sender selects an appropriate transmission mode for sending an outgoing message from the plurality of transmission modes based on factors such as the recipient's messaging format capabilities information, and optionally the recipient's current registration/presence on a SIP network that implements an IM service and the sender's current registration status on the packet data network 102. *Supra*, §VII.C, §VIII.A, Analyses of Elements [1a2]-[1a3], [1b1]-[1b3].

78. In the combination, Horvath's sender wireless device 106 also includes an "SMS delivery network selector 124" that "selects a network 102, 104 for the wireless device 106 to transmit a SMS message on," based on the network registration status of the sender wireless device 106. APPLE-1004, [0062] ("[I]f the wireless device 106 is registered on the packet data network 102, the SMS delivery network selector 124 selects the packet data network 102 for transmission of the SMS message. If the wireless device is not registered on the packet data network 102, the SMS delivery network selector 124 selects the circuit services network 104 for transmission of the SMS message."), FIGS. 1, 2, 4 (below). Sender wireless device 106 can also select a format for an outgoing message, at least partially based on the specific messaging service(s) it has subscribed with and is thus capable of using. APPLE-1004, [0039] ("An IMS system also includes application servers that host and execute services for the wireless device 106. A service for example, is SMS, MMS, caller ID, call waiting, push-to-talk, voicemail, and the like.").

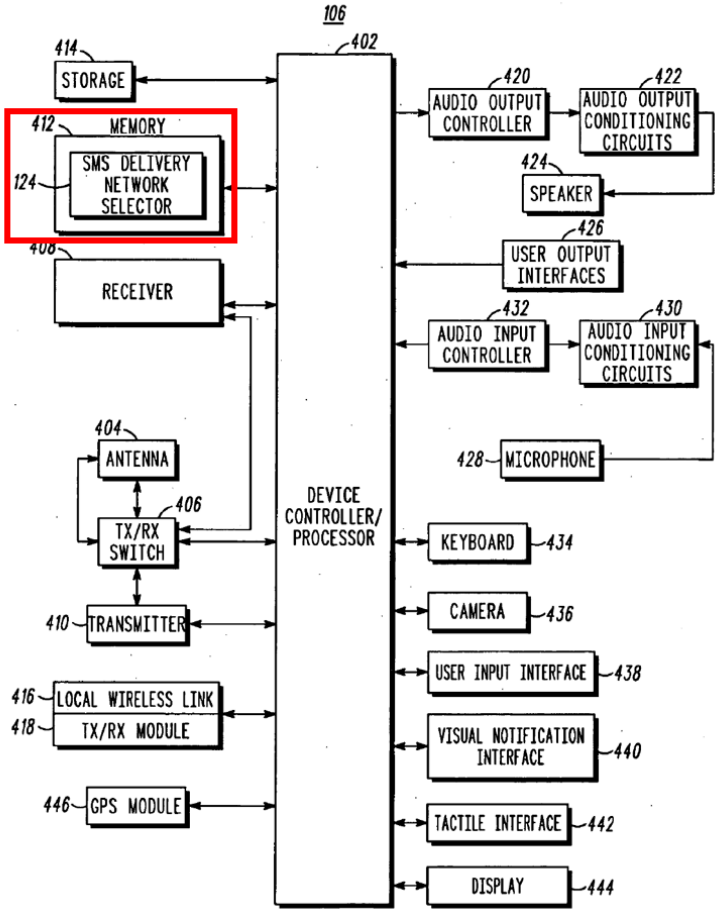


FIG. 4

APPLE-1004, FIG. 4 (Annotated)

79. Tsampalis additionally discloses a "send message circuitry 106" that "operates to send a message in a message format compatible with at least one of the formats identified in the [recipient device] messaging format capabilities information 110," and "sends message" "in a format identified in the [recipient device] messaging format capabilities information 110, to the network 108 via the transceiver 102." *See e.g.*, APPLE-1005, [0025], [0027], [0033], [0037] ("the send

message circuitry 106 formats the message prior to sending the message"), [0041], FIGS. 1, 2. As discussed above, a POSITA would have found it obvious to implement Horvath's system in accordance with Tsampalis's teachings such that the sender device in the Horvath-Tsampalis combination would select a transmission mode such as an MMS, IM, or SMS-based transmission mode based on factors such as the recipient's messaging format capabilities information, and optionally the recipient's current registration/presence on a SIP network that implements an IM service and the sender's current registration status on the packet data network 102. *Supra*, §VII.C, §VIII.A, Analyses of Elements [1a2]-[1a3], [1b1]-[1b3].

Element [1c2]: wherein the wireless device of the sender selects the first transmission mode when the indication corresponds to a subscriber of the service,

Element [1c3]: and the wireless device of the sender is capable of selecting the second transmission mode when the indication does not correspond to a subscriber of the service;

80. Horvath-Tsampalis renders obvious [1c2]-[1c3]. As discussed above in connection with elements [1a2]-[1a3], the wireless device of the sender in the Horvath-Tsampalis combination is configured to select an MMS-based or IM-based transmission mode (either of which corresponds to a ***first transmission mode***) when the sender determines based on the recipient's messaging format capabilities information that the recipient is capable of receiving/processing MMS or IM

messages. *Supra*, §VII.C, §VIII.A, Analyses of Elements [1a2]-[1a3]. For example, Tsampalis teaches that a rich media format such as MMS can be set as the default format, and starting from Horvath's system which offers at least two rich media formats (MMS and IM), it would have been obvious for the sender device in the Horvath-Tsampalis combination to set MMS or IM as the default messaging format to benefit from the enhanced capabilities of those formats over SMS. APPLE-1005, [0062], [0064]; *see also id.*, [0036]-[0037], [0048]-[0054], [0062], [0064], FIG. 11; *supra*, §VII.C, §VIII.A, Analyses of Elements [1a2]-[1a3], [1b1] and [1c1]. In the combination, and based on Tsampalis's teachings, the Horvath-Tsampalis sender wireless device would select the default format (*e.g.*, MMS or IM) for transmitting an outgoing message according to a default transmission mode (*e.g.*, an MMS-based or IM-based transmission mode) when the recipient's messaging format capabilities information indicates that the recipient is a subscriber of an MMS or IM service for receiving messages via a packet switched bearer. *Supra*, §VIII.A, Analyses of Elements [1a2]-[1a3], [1b1]-[1b3]. In some examples, the sender device can also determine to send the outgoing message as an IM based on the recipient's current registration status/presence on a SIP network that implements an IM service. *Supra*, §VIII.A, Analysis of Element [1b3]. For example, the sender device may select an IM-based transmission mode when the recipient is currently online. *Id.* In some cases, it would have been

obvious that the sender wireless device would select the default format (*e.g.*, MMS or IM) for transmitting an outgoing message according to a default transmission mode (*e.g.*, an MMS-based or IM-based transmission mode) whenever the recipient's messaging format capabilities information indicates that the recipient is a subscriber of an MMS or IM service for receiving messages via a packet switched bearer.

81. Likewise, based on Tsampalis's teachings, the Horvath-Tsampalis sender wireless device selects the non-default format (e.g., SMS) for transmitting an outgoing message according to a non-default transmission mode (e.g., an SMS-based transmission mode) (***second transmission mode***) when the recipient's messaging format capabilities information indicates that the recipient has limited messaging capabilities and is therefore not a subscriber to the MMS or IM services that deliver messages via a packet switched bearer. APPLE-1005, [0062], [0064]; *see also id.*, [0036]-[0037], [0048]-[0054], [0062], [0064], FIG. 11; *supra*, §VII.C, §VIII.A, Analyses of Elements [1a2]-[1a3], [1b1] and [1c1]. Based on Horvath's teachings, the sender device in the Horvath-Tsampalis combination would send an SMS message in an SMS-based transmission mode over either the packet data network 102 or the circuit services network 104 depending on whether the sender device was registered with the packet data network 102 at the time of sending the message. APPLE-1004, [0050], [0078], FIG. 7.

Element [1d]: sending, by the wireless device of the sender, the outgoing message using the selected transmission mode,

82. Horvath-Tsampalis renders obvious [1d]. As discussed above, Horvath-Tsampalis's wireless device of the sender sends the outgoing message using the selected transmission mode. *Supra*, §VII.C, §VIII.A, Analyses of Elements [1a3] and [1c1]-[1c3].

Element [1e]: wherein, when the selected transmission mode is the first transmission mode, the wireless device of the sender sends the outgoing message as one or more Internet protocol (IP) packets to the wireless device of the recipient via the packet switched WLAN base station,

83. Horvath-Tsampalis renders obvious [1e]. As discussed above, when the selected transmission mode is the first transmission mode, the wireless device of the sender sends the outgoing message as an MMS or IM message over the packet data network 102, which Horvath explains "is an Internet Protocol ('IP') connectivity network," and which includes sending the MMS or IM message via a packet switched WLAN base station (*e.g.*, an IEEE 802.11 access point). APPLE-1004, [0024] (packet data network 102 is an Internet Protocol ("IP") connectivity network" and can include an "802.11 network"), [0034] ("runs over the standard IP"), FIGS. 1-2; *supra*, §VII.C, §VIII.A, Analyses of Elements [1a3], [1b1]-[1b3], and [1c1]-[1c3].

84. A POSITA also would have understood from Horvath's disclosure, or at least found obvious, that the WLAN base station (e.g., the IEEE 802.11 access

point) would be used for transmitting IP packets since the outgoing message is transmitted over a packet based network 102 that routes IP packets across the network to a recipient device. *Supra*, Analyses of Elements [1b1]-[1b3]; *see also* APPLE-1004, [0034] ("IMS is a Next Generation Networking architecture for mobile and fixed IP services. IMS uses a Voice-over-IP implementation and runs over the standard IP. The wireless device 106 can connect to the IMS network using different methods, which all use standard IP. For example, when a wireless device 106 wants to access the packet data network 102, the wireless device 106 registers with the IMS network. The basic functions of an IMS network should be known to those or ordinary skill in the art."). Consistent with these teachings, it would have been obvious that whenever the selected transmission mode is the first transmission mode, the wireless device of the sender can send the outgoing message as one or more Internet protocol (IP) packets to the wireless device of the recipient via the packet switched WLAN base station.

Element [1f]: wherein, when the selected transmission mode is the second transmission mode, the wireless device of the sender sends the outgoing message as a short message service (SMS) message to the wireless device of the recipient using the destination address via a base station that is associated with a cellular core network that is independent of the packet switched WLAN base station, and

85. Horvath-Tsampalis renders obvious [1f]. As discussed above, the sender wireless device in the Horvath-Tsamaplis combination selects SMS as a non-default format for transmitting an outgoing message according to an SMS-

based transmission mode (***second transmission mode***) when the recipient's messaging format capabilities information indicates that the recipient has limited messaging capabilities and is not a subscriber to MMS or IM services (and/or the recipient is not currently present to receive IMs). APPLE-1005, [0062], [0064]; *see also id.*, [0036]-[0037], [0048]-[0054], [0062], [0064], FIG. 11; *supra*, §VII.C, §VIII.A, Analyses of Elements [1a2]-[1a3], [1b1] and [1c1]. Based on Horvath's teachings, the sender device sends the outgoing message as an SMS message over either the packet data network 102 or the circuit services network 104 depending on whether the sender device was registered with the packet data network 102 at the time of sending the message. APPLE-1004, [0050], [0078], FIG. 7. Whether the SMS message is sent over the packet data network 102 or circuit services network 104, the message is sent to the wireless device of the recipient via a base station that is associated with a cellular core network that is independent of the packet switched WLAN base station.

86. For example, when the sender device sends the SMS message over circuit services network 104, a POSITA would have understood that the SMS message would bypass the sender's WLAN network and the packet switched WLAN base station altogether. Horvath explains that the circuit services network 104 is distinct from the packet data network 102 (including the 802.11 WLAN network), and it would have been obvious to a POSITA that the 802.11 WLAN

base station would not be used to transmit an SMS message over the circuit services network 104. APPLE-1004, [0024] ("[T]he packet data network 102 is an Internet Protocol ("IP") connectivity network, which provides data connections at much higher transfer rates then [*sic*] a traditional circuit services network."), [0050] ("If the wireless device 106, is not registered on the packet data network 102, the wireless device 106 transmits the SMS messages using the traditional circuit services network method (for example, ANSI-41 procedures)."), [0025]-[0028], [0047], FIGS. 1-2. Based on Horvath, it would have been obvious that the sender device in the Horvath-Tsampalis combination would transmit an SMS message over the circuit services network 104 even after polling a server for messaging format capabilities information and/or presence information of the recipient over the packet data network 102 if the sender device subsequently "deregistered" or "lost its coverage" with respect to the packet data network 102. APPLE-1004, [0047]-[0049]. The SMS message transmitted over circuit services network 104 would be sent via a base station that is associated with a cellular core network that is independent of the packet switched WLAN base station, such as a base station of a CDMA or GSM cellular network. APPLE-1004, [0024]-[0026], FIGS. 1-2; *see also id.*, [0002], [0032], [0081] ("a base-station controller"), [0039] ("The present invention is not limited to the IS-41 based circuit network. Other networks such as a GSM map circuit network can also be used."); APPLE-1011, 1:32-34 ("a base

station includes but is not limited to a Node-B, site controller, access point or any other type of interfacing device in a wireless environment"), 2:44-48 ("cellular telephones" "having an appropriate card enabling communication with [a] WLAN access point (AP)"); APPLE-1014, [0006] ("cellular network (*e.g.*, GSM-global system for mobile communications)"), [0047] ("other cellular network technologies (*e.g.*, UMTS, CDMA…)"), [0108] ("The GSM network 1900 includes a base station subsystem (BSS) 1902, a network subsystem (NSS) 1904 and a GPRS core network 1906. The BSS 1902 can include one or more base transceiver stations (BTS) 1908 and a base station controller (BSC) 1910 connected together on an A-bis interface. The BTS and accompanying base stations (not shown) connect a cell phone to a cellular network. Base stations are all interconnected to facilitate roaming from one cell to another via a process called handover, without losing the cell connection."), FIG. 19); APPLE-1015, [0027] ("Base station 120, including its associated controller and antenna tower 118, provides wireless network coverage for a particular coverage area commonly referred to as a 'cell'. Base station 120 transmits communication signals to and receives communication signals from mobile stations within its cell via antenna tower 118. Base station 120 normally performs such functions as modulation and possibly encoding and/or encryption of signals to be transmitted to the mobile station in accordance with particular, usually predetermined, communication

protocols and parameters, under control of its controller. Base station 120 similarly demodulates and possibly decodes and decrypts, if necessary, any communication signals received from mobile station 102 within its cell."), FIG. 1.

87. Likewise, when the sender device sends the SMS message over data packet network 102 but the recipient is not registered with the SIP network on packet data network 102, the SMS message is still sent to the recipient device via a base station that is associated with a cellular core network independent of the packet switched WLAN base station. For example, Horvath explains that if the recipient is not registered, then "[t]he SMSC 114, at step 610, delivers the SMS message through the traditional circuit services network method (for example, ANSI-41 procedures)." APPLE-1004, [0075]-[0076], FIG. 6. In this case, SMS message is transferred from the SIP network to the circuit services network 104 and delivered via a base station associated with a cellular core of the circuit services network 104. *Id.*; *see also id.*, [0026]-[0028], FIGS. 1-2. Noticeably, the plain language of [1f] does not require that the SMS message is never processed by the packet switched WLAN base station. The claim language only requires use of a base station that is associated with a cellular core network that is independent of the packet switched WLAN base station at some point in the process of sending the SMS message to the recipient. Considering these teachings, it would have been obvious that whenever the selected transmission mode is the second transmission

mode, the wireless device of the sender can send the outgoing message as a short message service (SMS) message to the wireless device of the recipient using the destination address via a base station that is associated with a cellular core network that is independent of the packet switched WLAN base station.

Element [1g]: wherein the request sent to the server and the response received from the server do not traverse the cellular core network.

88. Horvath-Tsampalis renders obvious [1g]. As discussed above, the request sent to the server and the response received from the server are transmitted via the packet data network (*e.g.*, "an 802.11 network" which is Wi-Fi) by default to unburden the traditional circuit services network, and thus a POSITA would have understood and found obvious that neither the request nor the response traverse the cellular core network (*e.g.*, the circuit services network 104) since the Wi-Fi network and its connection to the Internet are not part of the cellular core network. APPLE-1004, [0021], [0024], [0034], [0039] ("IS-41 based circuit network 104… The present invention is not limited to the IS-41 based circuit network. Other networks such as a GSM map circuit network can also be used, as should be obvious to those of ordinary skill in the art"), [0050], FIGS. 1, 2; s*upra*, §VII.C, §VIII.A, Analyses of Elements [1b2]-[1b3] and [1f]; APPLE-1009, 1 (differentiating "GSM SMS text messaging and Internet Protocol (IP) based communication"), 2 ("Registration with the registration server will allow the possibility or option of delivering the message via an IP based route … If the IP

based route is not available, conventional GSM delivery of an SMS message… is attempted."), 4 ("GSM – Global System Mobile"). An IS-41 based circuit network is a type of cellular network. IS-41 (Interim Standard 41), also known as ANSI-41, is a mobile telecommunications standard primarily used in North America for messaging signaling, mobility, and roaming in cellular networks, particularly those based on AMPS, TDMA, and CDMA technologies.

Element [11pre]: A method of providing a messaging service for use in a wireless device of a sender, the method comprising:

89. *Supra*, §VIII.A, Analysis of Element [1pre].

90. Independent Claim 11 recites the same or similar limitations as Claim 1, thus Horvath-Tsampalis renders obvious Claim 11 for at least the same reasons as discussed above for Elements [1pre]-[1g] of Claim 1.

Element [11a1]: receiving, by a message client running on the wireless device of the sender, information associated with a destination address of a wireless device of a recipient,

91. *Supra*, §VIII.A, Analysis of Element [1a1].

Element [11a2]: the message client capable of determining a transmission mode for sending an outgoing message to the wireless device of the recipient,

92. *Supra*, §VIII.A, Analysis of Element [1a2].

Element [11a3]: wherein the wireless device of the sender is capable of sending messages in a plurality of transmission modes comprising a first transmission mode and a second transmission mode;

93. *Supra*, §VIII.A, Analysis of Element [1a3].

Element [11b1]: determining, by the wireless device of the sender, whether the destination address corresponds to a subscriber of a service for receiving the outgoing message via a packet switched bearer

94. *Supra*, §VIII.A, Analysis of Element [1b1].

Element [11b2]: by sending a request via a packet switched wireless local area network (WLAN) base station to a server,

95. *Supra*, §VIII.A, Analysis of Element [1b2].

Element [11b3]: and receiving a response from the server via the packet switched WLAN base station, the response providing an indication of whether the destination address corresponds to a subscriber of the service;

96. *Supra*, §VIII.A, Analysis of Element [1b3].

Element [11c1]: selecting, by the wireless device of the sender, a transmission mode for sending the outgoing message to the wireless device of the recipient from the plurality of transmission modes,

97. *Supra*, §VIII.A, Analysis of Element [1c1].

Element [11c2]: wherein the wireless device of the sender selects the first transmission mode when the indication corresponds to a subscriber of the service,

98. *Supra*, §VIII.A, Analysis of Element [1c2].

Element [11c3]: and the wireless device of the sender is capable of selecting the second transmission mode when the indication does not correspond to a subscriber of the service,

99. *Supra*, §VIII.A, Analysis of Element [1c3].

Element [11d]: wherein the wireless device of the sender is capable of sending, in the first transmission mode, the outgoing message as one or more Internet protocol (IP) packets to the wireless device of the recipient via the packet switched WLAN base station,

100. *Supra*, §VIII.A, Analyses of Elements [1d]-[1e].

Element [11e]: wherein the wireless device of the sender is capable of sending, in the second transmission mode, the outgoing message as a short message service (SMS) message to the wireless device of the recipient using the destination address via a base station that is associated with a cellular core network that is independent of the packet switched WLAN base station, and

101. *Supra*, §VIII.A, Analysis of Element [1f].

Element [11f]: wherein the request sent to the server and the response received from the server do not traverse the cellular core network.

102. *Supra*, §VIII.A, Analysis of Element [1g].

Claim [2]: The method of claim 1, further comprising: displaying, by the wireless device of the sender, a result of the indication of whether the destination address corresponds to a subscriber of the service.

Claim [12]: The method of claim 11, further comprising: displaying, by the wireless device of the sender, a result of the indication of whether the destination address corresponds to a subscriber of the service.

103. Horvath-Tsampalis renders obvious Claims [2] and [12]. For example, Horvath's wireless device has a "visual notification (or indication interface 440)" that "can be used as an alert by displaying a sequence of colored lights or a single flashing light on [a] display 444 or LEDs…when the wireless device 106 receives a message, or the user missed a call," where display 444 is "for displaying information to the user of the wireless device 106." APPLE-1004, [0068], [0070], FIG. 4 (below).

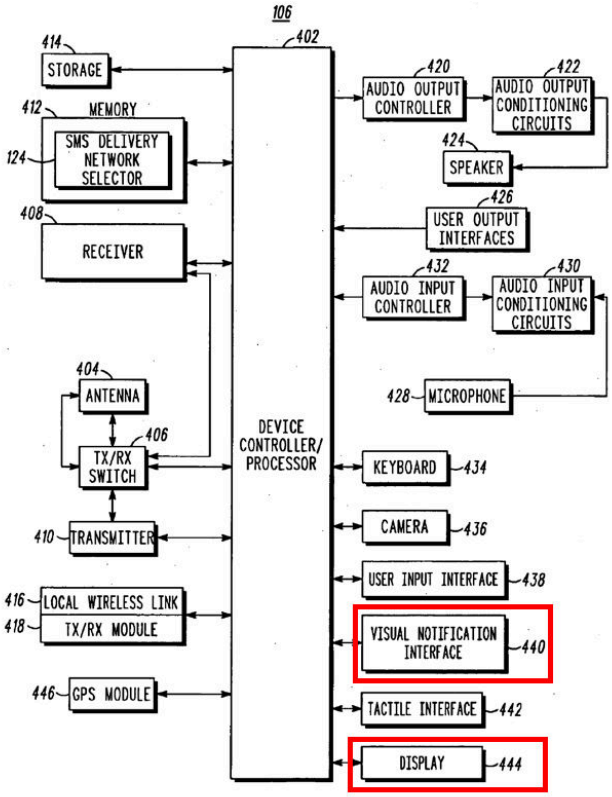


FIG. 4

APPLE-1004, FIG. 4 (Annotated)

104. Additionally, Tsampalis discloses that the sender device displays a "prompt" for the user to choose a message format based on obtained recipient device messaging format capabilities information, prior to sending a message. APPLE-1005, [0004], [0037] ("[T]he send message circuitry 106 sends, to the user interface 202, a prompt to the user (not shown). The prompt presents to the user a question as to whether the user would like the active message 216 formatted in a format identified in the recipient list messaging format capabilities 406 or whether the user would like the active message 216 sent to the recipient ID 402 in the

default messaging capability of the first mobile wireless communication device 100."), [0038] (sender device "prompts the user to select which among the [recipient device] messaging format capabilities information 110 to format the active message 216 in before sending the message 112"), [0052] ("each recipient in the active message recipient list that is flagged as not being compatible with the sending device's default messaging format....the method displays options to the user for each flagged recipient."), [0062] ("The [sender device] will also advice the user that any attached/inserted multimedia files will be lost, The [sender device] then prompts the user with the options to…"), [0065], FIG. 12 ("display options and input user selection").

105. In the combined system of Horvath-Tsampalis, it would have been obvious for the wireless device of the sender to display a result of the indication of whether the destination address corresponds to a subscriber of the service (*e.g.*, MMS or IM), in accordance with Tsampalis to provide an enhanced user experience by providing a "prompt" for the user of the sender device to choose a messaging format compatible with the recipient device. *Supra*, §VII.C, §VIII.A, Analyses of Elements [1b1]-[1b3], [1c1]-[1c3]; APPLE1013, 6:41-51 ("A platform indicator [displayed to the user] is to indicate to the user the original platform of the message. For example, it may be a voice mail, an email, an IM message..."), 7:29-34 ("For example, a platform indicator may indicate the original message

platform, or type of a message, such as email, SMS, or voice mail. A color or a visual shape may help the user identify the message type, and thus, help the user decide on a message platform to use for an outbound reply message."); APPLE1010, 16:15-21 ("Communication mode categories may be shown in an enabled or disabled state. A communication mode category may be shown in a disabled state if there are no available communication modes within the communication mode category. A communication mode category may be shown in an enabled state if there is at least one available communication mode within the communication mode category."), 17:43-46 ("Contact view 865 of FIG. 8D displays a synchronous text window 870 that presents available communication modes included in synchronous text communication mode category 835."), 21:40-46 ("At block 1315, enabled and disabled communication mode categories are displayed in a communication action bar. An enabled communication mode category may be displayed if there is at least one available communication mode within the communication mode category. If there are no available communication modes within the communication mode category, then a disabled state may be displayed."), FIGS. 8D, 13.

Claim [3]: The method of claim 1, further comprising: selecting, by the wireless device of the sender, at least one type of permissible attachment based on whether the destination address corresponds to a subscriber of the service.

Claim [13]: The method of claim 11, further comprising: selecting, by the wireless device of the sender, at least one type of permissible attachment based on whether the destination address corresponds to a subscriber of the service.

106. Horvath-Tsampalis renders obvious Claims [3] and [13]. As discussed above, the Horvath-Tsampalis wireless device is capable of determining and selecting a transmission mode for sending an outgoing message based on whether the destination address of the recipient device is associated with either MMS or IM messaging format capabilities (***corresponds to a subscriber of the service***). *Supra*, §VII.C, §VIII.A, Analysis of Claim [1].

107. For example, if the sender device selects the first transmission mode, *e.g.*, when both the sender and recipient devices have MMS (or IM in the alternative mapping) capabilities (***the destination address corresponds to a subscriber of the service***), then the sender device has the option of attaching at least one type of permissible attachment (*e.g.*, multimedia file(s) such as images, audio, video) with the outgoing message since MMS supports multimedia attachments. APPLE-1004, [0025], ("Multimedia Messaging Service ('MMS')"), [0029], [0068]-[0069] ("multimedia message" such as "a video media component"); APPLE-1005, [0062] ("the first mobile wireless communication device 100 [sender device] informs the associated user that the recipient (or recipients) have limited messaging capabilities [of only SMS], and suggests to the user to transform (format) the message to an SMS formatted message and send it.

The first mobile wireless communication device 100 will also advice the user that any attached/inserted multimedia files will be lost."); *supra*, §VII.C, §VIII.A, Analysis of Claim [1].

108. If the sender device selects the second transmission mode, *e.g.*, because the recipient device is only capable of SMS and not capable of either MMS or IM (***the destination address does not correspond[] to a subscriber of the service***), then the wireless device of the sender sends a text-only SMS message without any attachments, knowing that any attachment will be lost before reaching the recipient device.

Claim [4]: The method of claim 1, further comprising: denying, by the wireless device of the sender, when the destination address does not correspond to a subscriber of the service, any type of attachment.

Claim [14]: The method of claim 11, further comprising: denying, by the wireless device of the sender, when the destination address does not correspond to a subscriber of the service, any type of attachment.

109. Horvath-Tsampalis renders obvious Claims [4] and [14]. *Supra*, §VIII.A, Analysis of Claim [3]. As discussed above, in some examples, such as when the recipient is not a subscriber of an MMS or IM service and is unable to process or receive MMS or IM messages, Horvath-Tsampalis's wireless device of the sender denies any type of attachment, knowing that "any attached/inserted multimedia files will be lost," before reaching the recipient device. APPLE-1005, [0062].

Claim [5]: The method of claim 1, wherein the destination address is a mobile phone number.

Claim [15]: The method of claim 11, wherein the destination address is a mobile phone number.

110. Horvath-Tsampalis renders obvious Claims [5] and [15]. For example, as described above in the analysis of element [1a1], the destination address can be a mobile phone number. *Supra*, §VIII.A, Analysis of Element [1a1]; APPLE-1004, [0035], [0045]-[0046], [0050], [0073], [0076]; APPLE-1005, [0033], [0064], FIG. 4.

Claim [6]: The method of claim 1, further comprising: queuing the outgoing message for later delivery if the outgoing message cannot be delivered to the wireless device of the recipient.

Claim [16]: The method of claim 11, further comprising: queuing the outgoing message for later delivery if the outgoing message cannot be delivered to the wireless device of the recipient.

111. Horvath-Tsampalis renders obvious Claims [6] and [16]. For example, when the outgoing message is an SMS or MMS message, a remote server system implements "store-and-forward" capabilities in which the outgoing message is queued for later delivery if the message cannot be delivered to the wireless device of the recipient. APPLE-1005, [0022]-[0024] (explaining that SMS and MMS are "non-real time store-and-forward messaging" services); *supra*, §VIII.A, Analysis of Claim [1]. Moreover, queuing messages for later delivery if the outgoing message cannot be delivered as claimed (*e.g.*, due to the recipient's phone being offline, out of coverage, or having a full inbox) was a common practice and well-

known before the Critical Date. APPLE-1016, [0003] ("In order to receive an SMS message at the time it is sent, a user receiving the message must have his or her SMS capable mobile device, such as a wireless telephone, in his or her possession and the telephone must be turned on. If the telephone cannot be reached, for example, if it is turned off or if the battery is discharged, the message will be queued for later transmission."), [0020] ("an SMS message will simply be transmitted in the normal way and queued if the condition is such that the message cannot immediately be transferred to the [recipient] telephone"); APPLE-1009, FIG. 2 ("If the mobile device is not subscribed via IP, messages would be either be queued until the mobile device registers over an IP based route or after a set period the messages would be routed as a GSM SMS message."), page 2 ("if the handset is not registered with the registration server, the message will be queued for IP based delivery within a specified time period."); APPLE-1017, 34:66-35:33 ("the message may be held until the mobile phone is on line. In other words, when the user is logged in or when the presence of the user is detected, the message is delivered.").

Claim [7]: The method of claim 1, further comprising: receiving, by the wireless device of the sender, a delivery confirmation message, via the packet switched WLAN base station, if the outgoing message is successfully delivered to the wireless device of the recipient, when the destination address corresponds to a subscriber of the service.

Claim [17]: The method of claim 11, further comprising: receiving, by the wireless device of the sender, a delivery confirmation message, via the packet

switched WLAN base station, if the outgoing message is successfully delivered to the wireless device of the recipient, when the destination address corresponds to a subscriber of the service.

112. Horvath-Tsampalis renders obvious Claims [7] and [17]. For example, Horvath discloses a server that determines message delivery success based on "an acknowledgement" sent from the recipient device. APPLE-1004, [0076] ("The SMSC 114, at step 61S, determines if delivery of the SMS message though [*sic*] the packet data network was successful (i.e. has an acknowledgement been received)."), [0080], FIG. 8. Likewise, Tsampalis describes the transmission of "signal[s]" from a remote server to a sender device, such as "new capabilities signal two" from a remote relay/server to a local relay/server and then "new capabilities signal one" from the local relay/server to the first mobile wireless communication device (sender device), containing indicators of message delivery result. APPLE-1005, [0058] ("The new capabilities signal two 1322 is also shown to contain an MM_Status_Code 1406, X-MMS_Status_Code 1408, and in the case of where a message is failed to be delivered, the potential values include 'unrecognized' 1410 and 'unsupported message' 1412."), [0059] ("The new capabilities Signal one 1326 is also shown to contain an MM Status 1506, where the MM Status 1506 is further based on an X-MMS MM Status 1508, and in the case of where a message is failed to be delivered, the potential values include 'rejected' 1510 and 'unsupported message' 1412."), FIGS. 14, 15. A POSITA

would have understood that the sender's receipt of a signal that indicates a status other than unrecognized, unsupported, rejected, or the like, indicates that the outgoing message has been successfully delivered to the recipient device. *Id.*

113. A POSITA would have found obvious for Horvath-Tsampalis's sender device to receive a delivery confirmation message, *e.g.*, the remote server forwarding the received "acknowledgement" message to the sender device or sending a notification of successful or "failed"/"rejected" delivery to the sender device, which would allow the sender to attempt a re-transmission or re-formatting of the message to the extent needed to successfully deliver the message to the recipient. Moreover, it was common practice and well-known in the field of wireless communication for a sender device to receive a message delivery confirmation message when the outgoing message is successfully delivered to the recipient device. APPLE-1008, [0063] ("The receiving terminal (50) that receives the multimedia contents transmits to the transmitting terminal (10), a delivery report signal indicating that the contents have been received (S24)."); APPLE-1012, FIGS. 5, 6, 7 (steps 511, 612, 712, "send short message delivery report using SIP message'" to the IMS-based user equipment), FIG. 7 (step 712); APPLE-1018, 14-33 ("If this delivery service provides delivery confirmation (Block 745), the EMS may optionally choose to await confirmation (Block 750) before notifying the

sender of the message delivery (and, preferably, the mechanism used) at Block 755.").

114. As discussed above regarding the request sent to the server and the response to the request back from the server to the sender device, both transmitted via the packet switched WLAN base station (*e.g.*, Wi-Fi router), a POSITA would have understood and found obvious that the delivery confirmation message is also sent by the remote server to the sender device via the packet switched WLAN base station by default, to unburden the circuit services network, when the recipient device has MMS or IM capabilities (***subscriber of the service***) established by the SIP network. *Supra*, §VIII.A, Analyses of Elements [1b2]-[1b3].

Claim [8]: The method of claim 7, further comprising: displaying, by the wireless device of the sender, a delivery indication based on the received delivery confirmation message.

Claim [18]: The method of claim 17, further comprising: displaying, by the wireless device of the sender, a delivery indication based on the received delivery confirmation message.

115. Horvath-Tsampalis renders obvious Claims [8] and [18]. As discussed above, a POSITA would have found it obvious for Horvath-Tsampalis's sender device to receive a delivery confirmation message. *Supra*, §VIII.A, Analysis of Claims [7], [17]. A POSITA also would have found it obvious for Horvath-Tsampalis's sender device to display for the sender a delivery indication based on the received delivery confirmation message, *e.g.*, using Horvath's "visual

notification (or indication interface 440)" and display 444 that is "for displaying information to the user of the wireless device 106," to enhance user experience by providing the sender with feedback of whether the attempted delivery was successful and giving the sender the opportunity (*e.g.*, by a "prompt," in accordance with Tsampalis) to try another communication method and/or mode, or try again at a later time, to reach the recipient if the earlier message was rejected or lost. *Supra*, §VIII.A, Analysis of Claims [2], [12]; APPLE-1004, [0068], [0070], FIG. 4; APPLE-1005, [0004], [0037]-[0038], [0052], [0062], [0065], FIG. 12; APPLE-1012, FIGS. 5, 6, 7 ("send short message delivery report using SIP message'" to the IMS-based user equipment), FIG. 7 (step 712); APPLE-1018, 14-33 ("notifying the sender of the message delivery").

Claim [9]: The method of claim 1, further comprising: displaying, by the wireless device of the sender, sent messages and received messages, wherein sent messages are displayed with a first characteristic and received message are displayed with a second different characteristic so as to distinguish the sent messages from the received messages.

Claim [19]: The method of claim 11, further comprising: displaying, by the wireless device of the sender, sent messages and received messages, wherein sent messages are displayed with a first characteristic and received message are displayed with a second different characteristic so as to distinguish the sent messages from the received messages.

116. Horvath-Tsampalis renders obvious Claims [9] and [19]. Indeed, by the Critical Date of the '127 Patent, it would have been obvious for Horvath-Tsampalis's sender wireless device to display sent messages and received

messages using different characteristics to distinguish the sent messages from the received messages, with obvious user experience benefits.

117. Indeed, this conventional and common-sense feature was well-known before the Critical Date, and a POSITA would have implemented such feature to allow the user of the device to more readily differentiate sent versus received messages, consistent with Tsampalis's express objective of enhancing user experience. APPLE-1010, 11:37-46 ("Incoming and outgoing messages 415 and calls 420 may include one or more icons and/or text indicating a communication type. For example, text may indicate that a stored communication is an incoming call, an outgoing call, a voice note (V-note), a missed call, an unanswered call, etc. In the illustrated embodiment, each communication (e.g., message or call) includes a communication type icon 410. Examples of communication type icons 410 include a left facing arrow to represent outgoing calls [or messages], a right facing arrow to represent incoming calls [or messages]"), FIGS. 4A-4C; APPLE-1013, 7:61-8:38 (teaching of displaying "sender identity" with a message, along with "message platform," and use of different characteristics such as "different colors to draw attention to key information"), FIG. 4; *supra*, §VIII.A, Analysis of Claims [2], [12].

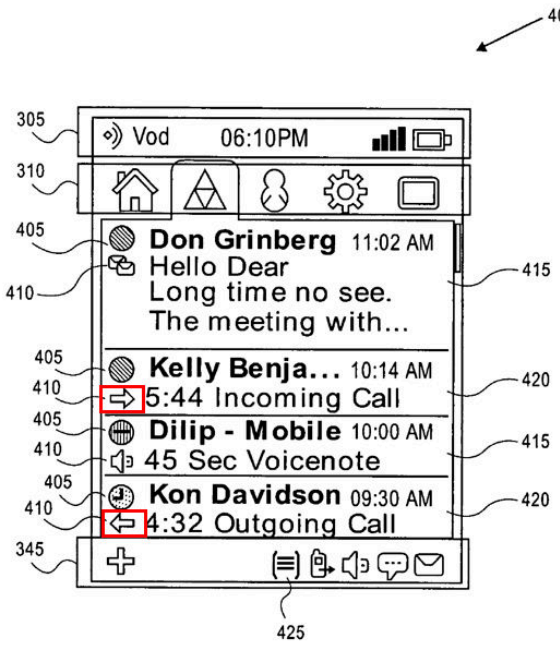


FIG. 4A

APPLE-1010 (Prior Art corroborating POSITA's Knowledge), FIG. 4A (Annotated)

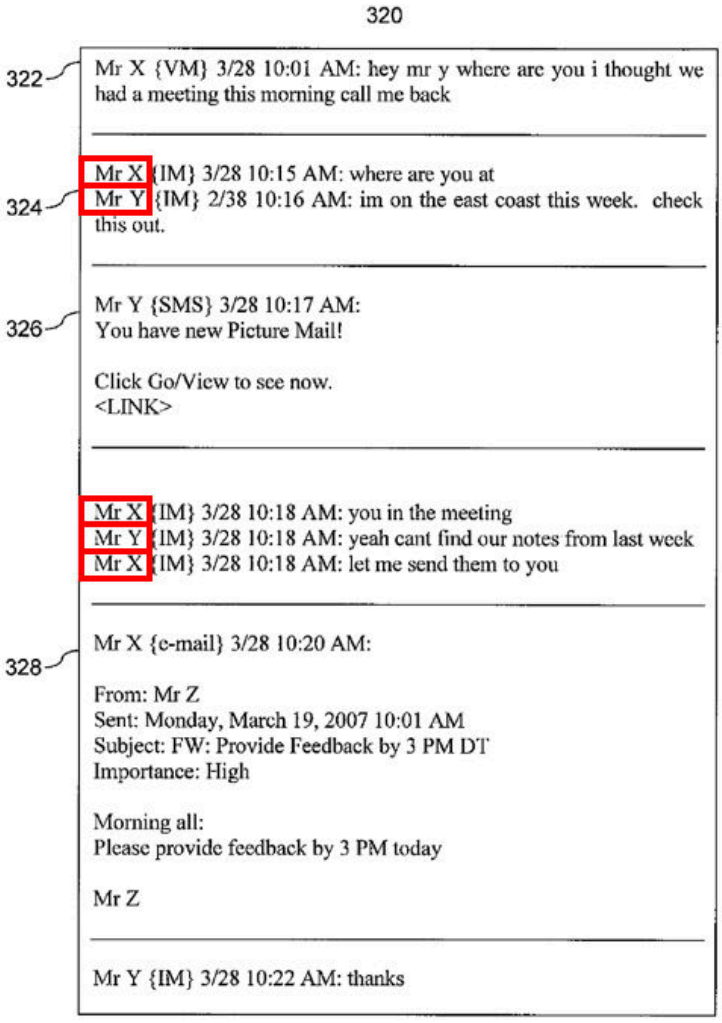


FIG. 4

APPLE-1013 (Prior Art Corroborating POSITA's Knowledge), FIG. 4

(Annotated)

Claim [10]: The method of claim 1, further comprising: receiving, by the wireless device of the sender, presence information associated with the wireless device of the recipient if the destination address corresponds to a subscriber of the service; and displaying, by the wireless device of the sender, the presence information associated with the wireless device of the recipient.

Claim [20]: The method of claim 11, further comprising: receiving, by the wireless device of the sender, presence information associated with the wireless device of the recipient if the destination address corresponds to a subscriber of

the service; and displaying, by the wireless device of the sender, the presence information associated with the wireless device of the recipient.

118. Horvath-Tsampalis renders obvious Claims [10] and [20]. As discussed above in connection with elements [1b1]-[1b3], it would have been obvious for the Horvath-Tsampalis sender device to receive presence information that indicates whether the intended recipient of an outgoing message is currently available to receive IMs (e.g., on a SIP network) if the destination address corresponds to a subscriber of an IM service. *Supra*, §VIII.A, Analysis of Elements [1b1]-[1b3]; APPLE-1004, [0004], [0081]; APPLE-1005, [0004], [0026], [0062], [0065].

119. When a recipient device has IM capabilities but is unavailable (an example of ***presence information associated with the wireless device of the recipient***), e.g., offline or online but busy, such presence status affects whether and how a message can be delivered to the recipient (*e.g.*, when a recipient is offline, an instant message would not be delivered successfully). In this context, a POSITA would have further found it obvious to configure the wireless device of the sender to display the recipient's presence status to inform a user of the sender device of the recipient's presence, thereby allowing the user to decide whether to send a SMS instead or to wait and try IM when the recipient device is back online—i.e., a common practice well known in the field by the Critical Date to enhance user experience and reduce unnecessary system overhead. *Supra*, §VIII.A,

Analyses of Claims [1]-[2], [12]; APPLE-1010, 8:51-9:12 ("Returning to FIG. 1B, presence logic component 188 determines presence status of destination users. Presence status indicates online status (e.g., offline, online and busy, online and available, etc.) for the destination user. In one embodiment, presence status of the destination user is determined using one or more instant messaging service (e.g., America Online® instant messenger (AIM), ICQ®, Yahoo® instant messenger, Microsoft® instant messenger, etc.). Therefore, if the destination user is logged into any one of the multiple instant messaging services, for example, presence logic component 188 may determine that the destination user is online. In another embodiment, presence status of the destination user is determined by querying a presence server provided by a cellular phone service. In yet another embodiment, in a peer-to-peer (P2P) IM network, presence status may be provided by one or more peers. Alternatively, presence status may be determined using a combination of instant messaging services, P2P IM networks and a presence server of a cellular phone service.... Once presence status is determined, the presence status may be presented to a user via user interface 195."), 11:24-36 ("Each incoming and outgoing message 415 and call 420 may include current presence status 405 of a remote sender or recipient of the message 415 or call 420. The presence status 405 presented in the unified inbox view 400 may be updated continuously, periodically, or upon user input. In one embodiment, a green icon indicates an online/available

presence, a red icon indicates an offline presence, and an orange icon indicates an online/busy presence. Alternatively, presence status 405 may be indicated in other ways (e.g., by color coding a name of the sender or recipient). Presence status 405 may also indicate additional presence information such as with customized messages and/or icons/images (e.g., away from keyboard, be right back, in meeting, etc.).”); APPLE-1013, 13:19-21 (display of “location or presence of the sender”); APPLE-1019, Abstract (“A system and method are directed towards providing a user interface (21) for controlling a communication mode for a client device (103). The interface enables user to set a presence and/or a communicaiton [*sic*] mode, which the client device communicates to other devices directly or via an intermidiary [*sic*] server (106). The presence generally reflects the user’s availability, communication capability, desire to communicate, and the like. The presence can be directly or indirectly associated with the communicaiton [*sic*] mode, which can comprise SMS, IM, email, voice, and the like[.] The interface includes a contact list and enables the user to select a mode to communicate with a contact. The communication modes associated with each contact can also be incorporated into and displayed (21 in an email address book. This interface also indicates the communication mode of each incoming and outgoing (228) message conversations with one or more other client devices.”); APPLE-1020, 1:40-45 (“An instant messaging server keeps track of the online status of each of its

subscribed users (often referred to as presence information), and when someone from a user's buddy list is online, the service alerts that user and enables immediate contact with the other user."), 2:5-9 ("There is thus a need for a better and more complete messaging solution (that enables immediate messaging like IM) that is designed for wireless mobile electronic devices that can take advantage of the 'always on' nature of a mobile station.").

IX. CONCLUSION

120. For all the reasons I have noted in the foregoing paragraphs, claims 1-20 of the ’127 Patent are obvious in view of the references discussed above.

121. I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

APPENDIX A

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
1889 Museum Rd,
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 . . . 12

II. RESEARCH AND CREATIVE SCHOLARSHIP 13
- A. Thesis . . . 13
- B. Published Journal Papers (Refereed) . . . 13
- C. Published Books and Parts of Books . . . 15
- D. Edited Proceedings . . . 15
- E. Conference Presentations . . . 15
  - E.1. Conference Papers with Proceedings (Refereed) . . . 15
  - E.2. Conference Presentations with Proceedings (Non-Refereed) . . . 22
  - E.3. Conference Presentations without Proceedings . . . 22
- F. Other . . . 22
  - F.1. Submitted Journal Papers . . . 22
  - F.2. Refereed Research Reports . . . 23
  - F.3. Software . . . 23
  - F.4. Published Papers (Non-Refereed) . . . 23
  - F.5. Books in Preparation . . . 23
  - F.6. Workshops and External Courses . . . 23
- G. Research Proposals and Grants (Principal Investigator) . . . 24
- H. Research Proposals and Grants (Contributor) . . . 26
- I. Research Honors and Awards . . . 28

III. SERVICE 29
- A. Professional Activities . . . 29
  - A.1. Memberships and Activities in Professional Societies . . . 29
  - A.2. Conference Committee Activities . . . 29
- B. On-Campus Committees . . . 30
  - B.1. University of Florida . . . 30
  - B.2. Georgia Tech . . . 31
- C. Special Assignments . . . 31
- D. Ph.D. Examining Committees . . . 31
- E. External Member of M.S. Examining Committee . . . 35
- F. Consulting and Advisory Appointments . . . 35
- G. Civic Activities . . . 35

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION 36
- A. Honors and Awards . . . 36
- B. Invited Conference Session Chairmanships . . . 36
- C. Professional Registration . . . 36
- D. Patents . . . 36
- E. Editorial and Reviewer Work for Technical Journals and Publishers . . . 37
- F. Expert Witness Services . . . 39

V. OTHER CONTRIBUTIONS 41
- A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia) . . . 41

B. Special Activities 45

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2008	Pennsylvania State University State College, PA *Dissertation:* Characterizing the Impact of Ridigity on the Security of Cellular Telecommunications Networks *Advisors:* 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 *Minors:* Biology, Business Admin	Computer Science

EMPLOYMENT HISTORY

Title	Organization	Years
Associate Chair for Research	University of Florida	*August 2018–Present*
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 2024	CNT 4007 Computer Networks 1	310	Revamped Course
Fall 2023	CIS 6930 Cellular and Mobile Network Security	19	New Topics
Fall 2022	CNT 5410 Computer and Network Security	75	New Topics
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

University of Florida

CNT 4007 Computer Networks 1: *Fall 2024.* Provided the first major overhaul to this course in a number of years. While I have relied on the same book used by other faculty, I have created new homeworks, projects, and slides to better represent the current state of computer networks. I have also significantly expanded the discussion of security in this course.

CIS 6930 Cellular and Mobile Network Security: *Fall 2018, 2023.* 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 (2G-5G), 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. 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.

CNT 5410 Computer and Network Security: *Fall 2014-2022.* 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.

Georgia Tech In addition to the above courses, I also developed the following course while serving as a faculty member at Georgia Tech.

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

Hadi Abdullah University of Florida
Fall 2016–Summer 2022
Evaluating the security of ML-driven voice interfaces. Now: Research Scientist at Visa Research

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.

Logan Blue University of Florida
Fall 2016–Summer 2022
Investigated biological feature reconstruction from voice recordings. Now: Research Scientist at Harbor Labs

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.

Cassidy Gibson University of Florida
Fall 2019–Spring 2025
Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.

Christian Peeters University of Florida
Fall 2016–Summer 2022
Develop techniques to detect and defend against call and message interception attacks in cellular networks. Now: Research Scientist at Harbor Labs

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. First: Assistant Professor at the University of Colorado Boulder. Now: Director, Global Cyber Intelligence at Walmart

Imani Sherman University of Florida
Fall 2018–Summer 2021
Developing usable interfaces against robocalls. Co-advised with Juan Gilbert. Now: Assistant Professor at the University of California, San Diego

Luis Vargas University of Florida
Fall 2016–Summer 2021
Developing techniques for network-based detection and mitigation of malware in a healthcare environment. Now: Data Scientist at the Alethia Group

2. Ph.D. Students Supervised

Nathaniel Bennett University of Florida
Fall 2022–Present
Finding vulnerabilities in cellular core networks via fuzzing.

Seth Layton University of Florida
Fall 2020–Present
Detecting deepfakes in audio samples.

Allison Lu University of Florida
Fall 2022–Present
Measuring repeatability in computer security.

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

Tyler Tucker University of Florida
Fall 2021–Present
Evaluating the security of Bluetooth/cellular radios.

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.

Ryon Kennedy University of Florida
Fall 2020–Spring 2023
Finding vulnerabilities in cellular core networks via fuzzing. Left to join UFIT.

Eric (Yu) Liu Georgia Institute of Technology
Fall 2008
Research on the spread of malcode 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 Raytheon

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 University of Florida
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–Spring 2021
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. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022. (Acceptance rate: 24%).

2. 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.

3. Patrick Traynor, Kevin Butler, Jasmine Bowers, and Bradley Reaves. FinTechSec: Addressing the Scurity Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.

4. Nolen Sciafe, Henry Carter, Rachel Jones, Lyrissa Lidsky, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. *International Journal of Information Security (IJIS)*, 2017.

5. 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 Seurity (TOPS)*, 2017.

6. Henry Carter and Patrick Traynor. OPFE: Outsourcing Computation for Private Function Evaluation. *International Journal of Information and Computer Security (IJICS)*, 2017.

7. 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.

8. 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.

9. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor. Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing (TMC)*, To Appear 2016.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

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

22. 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.

23. Patrick Traynor. Securing Cellular Infrastructure: Challenges and Opportunities. *IEEE Security & Privacy Magazine*, 7(4), 2009.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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 Papers with Proceedings (Refereed)

1. Cassidy Gibson and Daniel Olszewski and Natalie Grace Brigham and Anna Crowder and Kevin R. B. Butler and Patrick Traynor and Elissa M. Redmiles and Tadayoshi Kohno. Analyzing the AI Nudification Application Ecosystem. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.

2. Tyler Tucker, Nathaniel Bennett, Martin Kotuliak, Simon Erni, Srdjan Capkun, Kevin Butler, and Patrick Traynor. Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).

3. Magdalena Pasternak, Kevin Warren, Daniel Olszewski, Susan Nittroueri, Patrick Traynor, and Kevin Butler. Characterizing the Impact of Audio Deepfakes in the Presence of Cochlear Implant Simulated Audio. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).

4. Anna Crowder, Daniel Olszewski, Patrick Traynor, and Kevin R. B. Butler. I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data Using Statistical Techniques. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2024. (Acceptance Rate 21.8%).

5. Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa Redmiles, Eakta Jain, Patrick Traynor, and Kevin Butler. "I Had Sort of a Sense that I Was Always Being Watched... Since I Was": Examining Interpersonal Discomfort From Continuous Location-Sharing Applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).

6. Nathaniel Bennett, Weidong Zhu, Benjamin Simon, Ryon Kennedy, William Enck, Patrick Traynor, and Kevin Butler. RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).

7. Kevin Warren, Tyler Tucker, Anna Crowder, Daniel Olszewski, Allison Lu, Caroline Fedele, Magdalena Pasternak, Seth Layton, Kevin Butler, Carrie Gates, and Patrick Traynor. Better Be Computer or I'm Dumb": A Large-Scale Evaluation of Humans as Audio Deepfake Detectors. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).

8. K. Virgil English, Nathaniel Bennett, Seaver Thorn, Kevin Butler, William Enck, and Patrick Traynor. Examining Cryptography and Randomness Failures in Open-Source Cellular Cores. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2024. (Acceptance rate: 21.3%)(Best Paper).

9. Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Carrie Gates, Kevin Butler, and Patrick Traynor. SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).

10. Imani Munyaka, Daniel Delgado, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. "I used to live in Florida": Exploring the Impact of Spam Call Warning Accuracy on Callee Decision-Making. In *Symposium on Usable Security and Privacy (USEC)*, 2024.

11. Jianliang Wu, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).

12. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti Ukirde, Kevin Butler, and Patrick Traynor. "Get in Researchers; We're Measuring Reproducibility": A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2023. (Acceptance rate: 19.8%).

13. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations. In *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, 2023. (Acceptance rate: 21%).

14. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023. (Acceptance rate: 14%).

15. Hadi Abdullah, Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke Bauer, Vincent Bindschaedler, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Symposium on Network and Distributed System Security (NDSS)*, 2023. (Acceptance rate: 16%).

16. Daniel Olszewski, Sandeep Sathyanarayana, Weidong Zhu, Kevin Butler, and Patrick Traynor. HallMonitor: A Framework for Identifying Network Policy Violations in Software. In *IEEE Conference on Communications and Network Security (CNS)*, 2022.

17. Hadi Abdullah, Aditya Karlekar, Vincent Bindschaedler, and Patrick Traynor. Demystifying Limited Adversarial Transferability in Automatic Speech Recognition Systems. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2022. (Acceptance rate: 32%).

18. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2022. (Acceptance rate: 17.2%).

19. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin R. B. Butler. FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware. In *Symposium on Network and Distributed System Security (NDSS)* , 2022. (Acceptance rate: 16.2%).

20. 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. (Acceptance rate: 18.2%).

21. Hadi Abdullah, Muhammad Sajidur Rahman, Christian Peeters, Cassidy Gibson, Washington Garcia, Vincent Bindschaedler, Thomas Shrimpton, and Patrick Traynor. Beyond L_p Clipping: Equalization based Psychoacoustic Attacks against ASRs. In *The Asian Conference on Machine Learning (ACML)*, 2021.

22. 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 Comunications Information and Internet Policy (TPRC 49)*, 2021.

23. 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. (Acceptance rate: 12.1%).

24. 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. (Acceptance rate: 12.1%).

25. 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.

26. 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%).

27. 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 *Procedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, 2019. (Acceptance Rate: 17.0% for full papers).

28. 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).

29. 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%).

30. 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%).

31. 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%).

32. 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%).

33. 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%).

34. 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%.

35. 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%.

36. 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%.

37. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szajda, and Patrick Traynor. Mitigating Risk while Complying with Data Retention Laws. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2018.

38. Logan Blue, Luis Vargas, and Patrick Traynor. Hello, Is It Me You're Looking For? Differentiating Between Human and Electronic Speakers for Voice Interface Security. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2018.

39. 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%).

40. 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%).

41. 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%).

42. 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%).

43. 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%).

44. 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%).

45. 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%).

46. 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%).

47. 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%).

48. 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%).

49. 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%).

50. 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%).

51. 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%).

52. Nolen Sciafe, 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%).

53. 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%).

54. 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%).

55. 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%).

56. 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%).

57. 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%).

58. 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%).

59. 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%).

60. 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).

61. 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%).

62. 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).

63. 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).

64. 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%).

65. 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%).

66. 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%).

67. 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%).

68. 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%).

69. 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%).

70. 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%).

71. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDr0p: 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%).

72. 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%).

73. 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%).

74. 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%).

75. 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%).

76. 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%).

77. 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%).

78. 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%).

79. Italo Dacosta, Vijay Balasubramaniyan, 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%).

80. 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%).

81. 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%).

82. 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%).

83. 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).

84. 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%).

85. 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%).

86. 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%).

87. 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%).

88. 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%).

89. 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%).

90. 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%).

91. 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%).

92. 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. **Artus Protocol STTR Phase II - Extension**
   Sponsor: Office of Naval Research
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$300,000 over 2 years*
   Awarded: August 2023

2. **Testing Audio Deep Fake Detectors**
   Sponsor: Bank of America
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$150,000 over 1 year*
   Awarded: August 2023

3. **Testing Audio Deep Fake Detectors**
   Sponsor: Bank of America
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$274,000 over 2 years*
   Awarded: August 2021

4. **Deploying Defenses for Cellular Networks Using the AWARE Testbed**
   Sponsor: Department of Homeland Security: CISA:
   Investigator(s): Patrick Traynor (PI), Kevin Butler, Guofei Gu, Radu Stoleru, Walter Magnussen, P. R. Kumar
   Amount: *$3,100,000 over 4 years*
   Awarded: October 2019

5. **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

6. **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

7. **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

8. **Workshop: Addressing the Technical Security Challenges of Emerging Digital Financal Services**
   Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *$50,000 over 1 year*
Awarded: September 2017

9. **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

10. **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

11. **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

12. **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

13. **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

14. **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

15. **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

16. **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

17. **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

18. **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

19. **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

20. **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. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
Sponsor: NSF SaTC
Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franzi Roesner, Apu Kapadia, Eakta Jain.
Amount: *$7,500,000 for 5 years*
Awarded October 2022

2. **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

3. **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

4. **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

5. **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

6. **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

7. **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

8. **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

9. **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

10. **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

11. **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 co-Chair, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2023, 2024
2. Program co-Chair, *USENIX Security Symposium (SECURITY)*: 2019
3. Program co-Chair, *Network and Distributed System Security Symposium (NDSS)*: 2017, 2018
4. Program Chair, *USENIX Workshop on Offensive Technologies (WOOT)*: 2016
5. Program Chair, *ACM Conference on Wireless Network Security (WiSec)*: 2014
6. Program Co-Chair, *Annual Computer Security Applications Conference (ACSAC)*: 2012, 2013
7. Program Chair, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2012
8. Chair Invited Talks Committee, *USENIX Security Symposium (SECURITY)*: 2014
9. Workshops Chair, *IEEE Conference on Communications and Network Security (CNS)*: 2016
10. Program Committee, *USENIX Security Symposium (SECURITY)*: 2008, 2009, 2010, 2013, 2015-2018, 2020-2022
11. Program Committee, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2009-2014, 2022.
12. Program Committee, *ACM Conference On Computer and Communications Security (CCS)*: 2009, 2013-2015, 2017
13. Program Committee, *Network and Distributed System Security Symposium (NDSS)*: 2010, 2013-2016, 2020-2021
14. Program Committee, *IEEE European Symposium on Security and Privacy (Euro S&P)*: 2016
15. Program Committee, *Annual Computer Security Applications Conference (ACSAC)*: 2008, 2009, 2010, 2011, 2015
16. Program Committee, *ACM Conference on Wireless Network Security (WiSec)*: 2009, 2010, 2013, 2015-2021
17. Program Committee, *International Conference on Financial Cryptography and Data Security (FC)*: 2010, 2013
18. Program Committee, *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*: 2016.
19. Program Committee, *ICST Conference on Security and Privacy in Communication Networks (SecureComm)*: 2009, 2010
20. Program Committee, *Privacy Enhancing Technologies Symposium (PETS)*: 2015, 2016

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

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 Kanuparthy, 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. Patrick G. Traynor, Christian Peeters, Bradley G. Reaves, Hadi Abdullah, Kevin Butler, Jasmine Bowers, Walter N. Scaife, "Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding", United State Patent # 11,265,717, Filed March 2019, Issued March 2022.
2. Patrick G. Traynor, Logan E. Blue, Luis Vargas, "Method and Apparatus for Differentiating Between Human and Electronic Speaker for Voice Interface Security", United State Patent # 11,176,960, Filed June 2019, Issued November 2021.
3. Patrick G. Traynor, Bradley G. Reaves, Logan E. Blue Practical End-to-End Cryptographic Authentication for Telephony Over Voice Channels, United State Patent # 11,329,831, Filed November 2018, Issued May 2022.

4. 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)

5. 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.

6. 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.

7. 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.

8. 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)

9. 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. *ByteDance Ltd. vs CellSpin Soft, Inc.:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Ongoing. *February 2024 - Present*.
2. *Bank of America, N.A., vs PACid:* Expert witness for the Plaintiff for Inter Partes Review (via McNish PLLC). Status: Settled. *December 2023 - March 2024*.
3. *Microsoft vs Proxense, LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Ongoing. *November 2023 - Present*.
4. *Samsung vs Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Ongoing. *August 2023 - Present*.
5. *Advanced Coding Technologies LLC v. ByteDance PTE. Ltd., and TikTok PTE. Ltd.:* Expert witness for the Defense for Non-Infringement (via Fish & Richardson, LLP). Status: Dismissed with Prejudice. *July 2023 - September 2023*.
6. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021:* Expert witness for the Defendant (via Corrs Chambers Westgarth). Status: Ongoing. *January 2023 - June 2024*.
7. *Rubin vs KAHOOT! ASA and KAHOOT EDU:* Expert witness for the Defendant for Inter Partes Review (via Vasquez Benisek & Lindgren, LLP). Status: Ongoing. *December 2022 - June 2024*.
8. *Telefonaktiebolaget LM Ericsson vs Apple, Inc:* Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). Status: Settled. *February 2022 - December 2022*.
9. *Wepay Global Payments, LLC v. Bank of America N. A.,:* Expert Witness for the Defendant (via WilmerHale LLP) Status: Dismissed. *September 2022 - November 2022*.
10. *Apple vs. R.N Nehushtan Trust Ltd.:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Petition Denied. *August 2022 - June 2023*.
11. *Apple/Microsoft vs. Zipit Wireless:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Settled. *May 2021 - November 2022*.
12. *Blackberry Inc v MobileIron, Inc:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Settled. *January 2021 - March 2021*.

13. *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.*

14. *mSIGNIA, Inc. v. InAuth, Inc.:* Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity, Trade Secrets (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018*.

15. *Huawei v. T-Mobile:* Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017*.

16. *Telefonaktiebolaget LM Ericsson v Apple:* Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015*.

17. *Mayfonk v Nike:* Expert Witness for the Plaintiff for Infringement/Trade Secrets (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015*.

18. *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.*

19. *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.*

20. *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.*

21. *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.*

22. *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.*

23. *Intellectual Ventures LLC vs. Check Point; et al.:* Expert Consultant for the Plantiff 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. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. Learning from Authoritative Security Experiment Results (LASER) Workshop, December 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).

2. Social Engineering and Two-Factor Authentication. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).

3. DFS Security and Mobile Money Analysis. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).

4. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. EPFL Summer Research Institute (SURI), July 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).

5. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. North Central Florida Institute of Internal Auditors (IIA), May 2024.

6. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. UF Quest 2: Siri is my Superpower: Communicating with AI, March 2024. University of Florida.

7. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. Federal Information Integrity Research and Development (FIIRD) Interworking Group (IWG), March 2024. via NITRD, OSTP.

8. AI driven voice cloning scams. Discussion at the White House with Anne Neuberger (Deputy National Security Advisor for Cyber and Emerging Technologies), Jessica Rosenworcel (Chair of the Federal Communications Commission) and Lina Khan (Chair of the Federal Trade Commission), January 2024. Lead Academic facilitator.

9. Keynote: Well, It Worked on My Computer: Reproducibility, Tech Transfer, and Computer Security Research. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) Vision 2.0 Workshop, March 2023. University of Texas at Dallas.

10. Humans vs The Computer Interfaces: Separating Deepfakes/Bots from People Using Psychoacoustics. UCLA Electrical and Computer Engineering Distinguished Seminar, February 2023. University of California, Los Angeles.

11. Keynote: Exploiting the Gaps Between Human and Machine Understanding of Audio: Frameworks, Attacks, and Defenses. ISCA Symposium on Security and Privacy in Speech Communication (SPSC), November 2021. Virtual.

12. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.

13. 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.

14. 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.

15. 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.

16. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.

17. 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.

18. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.

19. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.

20. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweeden.

21. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejon, South Korea.

22. 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.

23. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.

24. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.

25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.

26. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.

27. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.

28. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.

29. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.

30. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.

31. 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.

32. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.

33. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.

34. 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.

35. 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.

36. 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.

37. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.

38. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.

39. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.

40. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.

41. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.

42. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.

43. 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.

44. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.

45. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.

46. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.

47. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.

48. 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.

49. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.

50. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.

51. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.

52. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.

53. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.

54. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.

55. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.

56. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.

57. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.

58. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.

59. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.

60. 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.

61. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.

62. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.

63. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.

64. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.

65. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.

66. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.

67. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.

68. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.

69. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.

70. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.

71. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.

72. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.

73. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.

74. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.

75. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.

76. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.

77. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.

78. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

79. 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. How technology can fight digital fakery. The Babbage Podcast/The Economist https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake, January 2023.

2. Deepfake audio has a tell and researchers can spot it. Ars Technica https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/, September 2022.

3. 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.

4. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255, July 2016.

5. 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.

6. Ransomware 'stopped' by new software. BBC - http://www.bbc.com/news/technology-36772461, July 2016.

7. Researchers create effective anti-ransomware solution. Help Net Security - https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/, July 2016.

8. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.

9. 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.

10. 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.

11. Desarrollan una solución para detener el ransomware. ComputerHoy - http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972, July 2016.

12. Why your antivirus software can't stop ransomware. Futurity - http://www.futurity.org/ransomware-computer-files-1198242-2/, July 2016.

13. 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.

14. 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-ransomeware-threat-071116.html, July 2016.

15. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - http://phys.org/news/2016-07-extortion-extinction-ransomware.html, July 2016.

16. 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.

17. 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.

18. 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.

19. 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.

20. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198, December 2013.

21. 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.

22. 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.

23. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399, October 2013.

24. 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.

25. 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.

26. Jim Burress. 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.

27. 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.

28. 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.

29. 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.

30. 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/#ixzz2EGtQsuLd, December 2012.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - http://www.technologyreview.com/computing/38913/?p1=A2, October 2011.

38. 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.

39. 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.

40. 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.

41. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - http://www.popsci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks, October 2010.

42. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.

43. 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.

44. 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.

45. 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.

46. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - ihttp://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.

47. 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.

48. 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.

49. 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.

50. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html, November 2009.

51. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11 /2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.

52. 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.

53. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/, June 2009.

54. 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.

55. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - http://www.uwire.com/Article.aspx?id=3738798, February 2009.

56. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - http://www.npr.org/templates/story/story.php?storyId=99790788, January 2009.

57. 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.

58. 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.

59. Associated Press. Hackers Expected To Start Targeting Cell Phones. http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html, 2008.

60. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.

61. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.

62. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.

63. 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/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.

64. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx, 2008.

65. 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.

66. Jamming Cellphones with Text Messages. Slashdot http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172, 2005.

67. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.

68. 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.