UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

Case No. IPR2026-00271
Patent No. 9,491,564

DECLARATION OF DR. PATRICK G. TRAYNOR

Google Exhibit 1003
Google v. Headwater

TABLE OF CONTENTS

I. PERSONAL AND PROFESSIONAL BACKGROUND 1

II. MATERIALS REVIEWED AND CONSIDERED 5

III. MY UNDERSTANDING OF PATENT LAW 8

A. Anticipation 10

B. Obviousness 10

IV. PERSON OF ORDINARY SKILL IN THE ART ("POSA") 13

V. THE '564 PATENT 15

A. Brief Description 15

B. Prosecution History of the '403 Patent 16

C. Grounds for Unpatentability 17

VI. CLAIM INTERPRETATION 18

VII. GROUND 1: TS-23.140 AND RAKIC RENDER OBVIOUS CLAIMS 1, 3-6, AND 11-21 19

A. TS-23.140 (EX-1004) 19

B. Rakic (EX-1007) 23

C. The MMS-Rakic Combination 28

1. Implementing TS-23.140's User Device with a Modem 28

2. Securing Interface MM1 Using SSL/TLS 33

3. Implementing TS-23.140's User Device with an Interprocess Communication Bus 37

4. Applying Rakic's Message Validation Techniques 41

5. MMS-Rakic 46

D. Claim Analysis 47

1. Claim 1 47

a. [1PRE] A mobile end-user device comprising: 47

b. [1A] a wireless modem configurable to exchange data via a connection to a wireless network; 48

c. [1B1] an inter-process software communication bus providing secure communication between an executing

device link agent and respective executing processes for a plurality of software components,..... 52

i. "an executing device link agent" 52

ii. "respective executing processes for a plurality of software components" 55

iii. "an inter-process software communication bus providing secure communication between…"..... 58

d. [1B2] wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and..... 60

e. [1C] the device link agent, configured to..... 66

f. [1D1] maintain a secure message link through the wireless network and an Internet network to a message link server,..... 67

g. [1D2] the message link server operating a message service that receives messages over a network from a plurality of network functions,..... 74

h. [1E] 78

i. receive secure messages from the message link server over the secure message link 78

ii. the received messages identified for delivery to multiple ones of the software components, and..... 79

iii. including message content received by the message link server from multiple ones of the network functions, and..... 80

i. [1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component..... 85

2. Claim 2: The mobile end-user device of claim 1, wherein the access authorization information provided by the secure server

for a given one of the software components comprises a signature. 87

3. Claim 3: The mobile end-user device of claim 1, wherein the software components include a first device component that receives message content in a first format, and a second device component that receives message content in a second format different than the first format. 87
4. Claim 4: The mobile end-user device of claim 3, further comprising a user interface, wherein the first device component is a user service interface agent, and the first format comprises a notification message, the user service interface agent configured to display the notification message on the user interface. 89
5. Claim 5: The mobile end-user device of claim 4, the user service interface agent further configured to obtain a user input as a response to the display of the notification message, and deliver the user input to an agent on the device. 93
6. Claim 6: The mobile end-user device of claim 3, wherein the first device component is a policy control agent, and the first format contains service settings and/or configuration information. 95
7. Claim 7: The mobile end-user device of claim 1, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes. 100
8. Claim 8: The mobile end-user device of claim 7, wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling..... 101
9. Claim 10: The mobile end-user device of claim 1, wherein the device link agent is further configured to receive, from one or more of the authorized software components, upload messages, each of the upload messages identifying a corresponding one of the network functions to which the device respective software component has requested delivery, the device link agent transmitting the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements..... 102

10. Claim 12: The mobile end-user device of claim 1, wherein at least one of the secure messages received from the network message server comprises multiple identifier/data pairs. 111

11. Claim 13: The mobile end-user device of claim 2, wherein the given one of the software components is identified by a secure unique identifier. 115

12. Claim 14 116

VIII. GROUNDS 2A-2C 116

A. GROUND 2A: MMS-Rakic in View of Cole (EX-1006) 117

B. GROUND 2B: MMS-Rakic in View of Sathish (EX-1031) 119

C. GROUND 2C: MMS-Rakic-Cole-Sathish 120

IX. GROUNDS 3A-3D 120

A. Ogawa (EX-1005) 121

B. GROUND 3A: Implementing Ogawa's Encryption Teachings 125

1. MMS-Rakic-Ogawa 125

a. Applying Ogawa's Symmetric Encryption Techniques 125

b. Ogawa's Decryption Unit 133

2. Claim 7: The mobile end-user device of claim 1, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes. 135

C. GROUNDS 3B-3D 136

X. GROUNDS 4A-4D 137

A. Ellison (EX-1019) 137

B. GROUND 4A: Implementing Ellison's Isolated Execution Environment (Claim 9) 141

1. MMS-Rakic-Ellison 141

2. Claim 9: The mobile end-user device of claim 1, wherein the device link agent executes in a secure execution environment, and at least one of the software components executes outside of the secure execution environment. 145

C. GROUNDS 4B-4D 146

XI. GROUNDS 5A-5D 147
A. Shen (EX-1027) 147
B. GROUND 5A: Implementing Shen's Heartbeat Teachings 148
1. MMS-Rakic-Shen 148
2. Claim 11 152
C. GROUNDS 5B-5D 153
XII. CLAIM LISTING APPENDIX 154

I, Patrick Gerard Traynor, declare:

1. I have been retained by Wolf, Greenfield & Sacks, P.C., counsel for Petitioner Google LLC to assess claims 1-14 (the "challenged claims") of U.S. Patent No. 9,491,564 ("the '564 patent"). My compensation is not dependent in any way upon the outcome of the *inter partes* review of the '564 patent.

I. PERSONAL AND PROFESSIONAL BACKGROUND

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 Interim Chair for 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 and messaging. 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. My dissertation concentrated on security issues in messaging for cellular systems.

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 have served 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 also previously served as the Security Subcommittee Chair for the ACM US Technology Policy Committee (USACM). I currently serve as an Associate Editor for ACM Transactions on AI Security and Privacy (TAISP).

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, blocking ransomware from encrypting data, and more.

14. My curriculum vitae, included with this declaration, 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. My curriculum vitae is provided as Appendix A.

II. MATERIALS REVIEWED AND CONSIDERED

16. My findings, as explained below, are based on my years of education, research, experience, and background in the field of services and application implementation in communication networks, as well as my investigation and study of relevant materials for this declaration. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art ("POSA"), as set forth in Section IV below. In forming my opinions, I have studied and considered the materials identified in the list below.

Exhibit	Description
1001	U.S. Patent No. 9,491,564 ("the '564 Patent")
1002	Prosecution History of U.S. Patent No. 9,491,564 ("the '564 FH")
1004	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 ("TS-23.140")
1005	U.S. Patent No. 8,195,961 ("Ogawa")
1006	U.S. Patent App. Pub. No. 2008/0080458 ("Cole")
1007	U.S. Patent App. Pub. No. 2009/0282256 ("Rakic")
1008	PCT Pub. No. 2008/048075 ("Lee")
1009	U.S. Pat. No. 7,975,147 ("Qumei")
1010	U.S. Pat. No. 9,032,192 ("Frank")
1011	Open Mobile Alliance; OMA-ERELD-MMS-v1_2-20030923-C, Enabler Release Definition for MMS Version 1.2," available at https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-ERELD-MMS-V1_2-20030923-C.pdf
1012	"Open Mobile Alliance; Multimedia Messaging Service Architecture Overview" (MMSARCH) specification, available at https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf
1013	The Secure Sockets Layer ("SSL") Protocol, V. 3.0, available at https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html and

	https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1
1014	The Transport Layer Security ("TLS") Protocol, V. 1.1, available at https://www.ietf.org/rfc/rfc4346.txt
1015	U.S. Patent App. Pub. No. 2003/0096625 ("Mi-Su Lee")
1018	Liaison Statement, European Telecommunications Standards Institute AT-F Rapporteur Meeting, 4 to 6 February 2003 (ETSI / AT-F TD18), available at https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_19/Docs/PDF/SP-030167.pdf
1019	U.S. Patent No. 7,082,615 ("Ellison")
1020	3GPP TS-26.140 v6.2.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Messaging Service(MMS); Media formats and codecs
1021	Multimedia Messaging Service Encapsulation Protocol, available at www.openmobilealliance.org/release/MMS/V1_2-20050301-A/OMA-MMS-ENC-V1_2-20050301-A.pdf
1022	*Samsung Elecs. et al. v. Headwater Research LLC*, IPR2024-00341, Paper 28 (July 23, 2025)
1023	Stewart, C.M., Memorandum Re: PTAB Consideration of Prior Findings of Fact and Conclusions of Law (September 16, 2025), https://www.uspto.gov/sites/default/files/documents/Memo_re_prior_findings_of_fact_and_conclusions_of_law_9_16_25.pdf.
1024	Declaration of Friedhelm Rodermund
1026	U.S. Patent App. Pub. No. 2005/0108571 ("Lu")
1027	U.S. Patent App. Pub. No. 2005/0207379 ("Shen")
1028	Transporting data between wireless applications using a messaging system—MMS, Miraj E Mostafa, Wireless Communications and Mobile Computing (2007) ("Mostafa")
1029	Dictionary of Computer Science, Engineering, and Technology, CRC Press LLC, 2001
1030	Needham et al., "Using Encryption for Authentication in Large Networks of Computers" (ACM, Vol. 21, No. 12, Dec. 1978) ("Needham")
1031	U.S. Patent No. 8,010,669 ("Sathish")
1032	Saltzer et al., "The Protection of Information in Computer Systems" (IEEE Proceedings, Vol. 63, No. 9, Sept. 1975) ("Saltzer")

1033	Li et al., "Symbian OS platform security model," available at https://www.usenix.org/system/files/login/articles/73507-li.pdf (Login Magazine, Aug. 2010)
1036	Schroeder et al., "A Hardware Architecture for Implementing Protection Rings" (ACM, Vol. 15, No. 3, Mar. 1972) ("Schroeder")
1037	Nokia E71 review: Nokia E71, available at https://www.cnet.com/reviews/nokia-e71-review/
1038	*Samsung Elecs. et al. v. Headwater Research LLC*, IPR2024-00341, Paper 4 (January 23, 2024)
1039	U.S. Patent App. Pub. No. 2007/0283170 ("Yami")
1040	U.S. Patent App. Pub. No. 2006/0077940 ("Ganji")
1041	U.S. Patent App. Pub. No. 2005/0282531 ("Andreasson")
1042	U.S. Patent App. Pub. No. 2003/0193967 ("Fenton")
1043	U.S. Patent App. Pub. No. 2004/0085894 ("Wang")
1044	U.S. Patent No. 6,094,424 ("Kalmanek")
1045	Dictionary of Computing, S.M.H. Collin, Fifth Edition, Bloomsbury (2004)
1046	IEEE 100 The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition (2000)
1047	U.S. Patent No. 7,962,798 to Locasto al. ("Locasto")
1048	U.S. Patent App. Pub. No. 2004/0002974 ("Kravitz")
1049	Computer Desktop Encyclopedia, Alan Freedman, Ninth Edition, Osborne/McGraw-Hill (2001)
1050	U.S. Patent No. 5,612,866 ("Savanyo")
1051	3GPP TS 25.321 v6.5.0 (2005-06); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Medium Access Control (MAC) protocol specification; ("TS-25.321")
1052	3GPP TS 25.322 v6.4.0 (2005-06); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Link Control (RLC) protocol specification; ("TS-25.322")
1053	3GPP TS 25.323 v5.4.0 (2005-06); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Packet Data Convergence Protocol (PDCP) specification; ("TS-25.323")
1054	Lu et al., Heading for Multimedia Message Service in 3G, 6th IEE International Conference on 3G and Beyond, Washington, D.C., USA, Nov. 7-9, 2005

1055	RFC 4355, IANA Registration for Enumservices Email, Fax, MMS, EMS, and SMS (Jan. 2006)
1056	Rodermund, A Picture Speaks a Thousand Words – From SMS to MMS, in Business Briefing: Wireless Technology (2003)
1057	U.S. Patent App. Pub. No. 2005/0091380 ("Gonen")
1058	U.S. Patent App. Pub. No. 2004/0258063 ("Raith")
1059	U.S. Patent App. Pub. No. 2004/0111476 ("Trossen")
1060	Prosecution History of U.S. Patent No. 9,232,403 ("the '403 FH")
1061	U.S. Patent App. Pub. No. 2007/0239898 ("Friend")
1062	U.S. Patent No. 7,269,433 ("Vargas")

III. MY UNDERSTANDING OF PATENT LAW

17. In developing my opinions, I discussed various relevant legal principles with Petitioner's attorneys. Though I do not purport to have prior knowledge of such principles, I understood them when they were explained to me and have relied upon such legal principles, as explained to me, in the course of forming the opinions set forth in this declaration. My understanding in this respect is as follows:

18. I understand that "*inter partes* review" (IPR) is a proceeding before the United States Patent & Trademark Office for evaluating the patentability of an issued patent's claims based on prior-art patents and printed publications.

19. I understand that, in this proceeding, Petitioner has the burden of proving that the challenged claims of the '564 patent are unpatentable by a preponderance of the evidence. I understand that "preponderance of the evidence" means that a fact or conclusion is more likely true than not true.

20. I understand that, in IPR proceedings, claim terms in a patent are given their ordinary and customary meaning as understood by a POSA in the context of the entire patent and the prosecution history pertaining to the patent. If the specification provides a special definition for a claim term that differs from the meaning the term would otherwise possess, the specification's special definition controls. If a claim element is expressed as a "means" for performing a specified function, I understand that it covers the corresponding structure described in the specification and equivalents of the described structure. I have applied these standards in preparing the opinions in this declaration.

21. I understand that determining whether a particular patent or printed publication constitutes prior art to a challenged patent claim can require determining the effective filing date (also known as the priority date) to which the challenged claim is entitled. I understand that for a patent claim to be entitled to the benefit of the filing date of an earlier application to which the patent claims priority, the earlier application must have described the claimed invention in sufficient detail to convey with reasonable clarity to the POSA that the inventor had possession of the claimed invention as of the earlier application's filing date. I understand that a disclosure that merely renders the claimed invention obvious is not sufficient written description for the claim to be entitled to the benefit of the filing date of the application containing that disclosure.

22. I understand that for an invention claimed in a patent to be patentable, it must be, among other things, new (novel—*i.e.*, not anticipated) and not obvious from the prior art. My understanding of these two legal standards is set forth below.

A. Anticipation

23. I understand that, for a patent claim to be "anticipated" by the prior art (and therefore not novel), each and every limitation of the claim must be found, expressly or inherently, in a single prior-art reference. I understand that a claim limitation is disclosed for the purpose of anticipation if a POSA would have understood the reference to disclose the limitation based on inferences that a POSA would reasonably be expected to draw from the explicit teachings in the reference when read in light of the POSA's knowledge and experience.

24. I understand that a claim limitation is inherent in a prior art reference if that limitation is necessarily present when practicing the teachings of the reference, regardless of whether a person of ordinary skill recognized the presence of that limitation in the prior art.

B. Obviousness

25. I understand that a patent claim may be unpatentable if it would have been obvious in view of a single prior-art reference or a combination of prior-art references.

26. I understand that a patent claim is obvious if the differences between the subject matter of the claim and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the relevant field at the time the invention was made. Specifically, I understand that the obviousness question involves a consideration of:

- the scope and content of the prior art;
- the differences between the prior art and the claims at issue;
- the knowledge of a person of ordinary skill in the pertinent art; and
- if present, objective factors indicative of non-obviousness, sometimes referred to as "secondary considerations." I have not been made aware of any secondary considerations asserted by Patent Owner ("PO") with respect to the '564 patent.

27. I understand that in order for a claimed invention to be considered obvious, a POSA must have had a reason for combining teachings from multiple prior-art references (or for altering a single prior-art reference, in the case of obviousness in view of a single reference) in the fashion proposed.

28. I further understand that in determining whether a prior-art reference would have been combined with other prior art or with other information within the knowledge of a POSA, the following are examples of approaches and rationales that may be considered:

- combining prior-art elements according to known methods to yield predictable results;
- simple substitution of one known element for another to obtain predictable results;
- use of a known technique to improve similar devices in the same way;
- applying a known technique to a known device ready for improvement to yield predictable results;
- applying a technique or approach that would have been "obvious to try," *i.e.*, choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success.
- known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
- some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior-art reference or to combine prior-art reference teachings to arrive at the claimed invention. I understand that this teaching, suggestion or motivation may come from a prior-art reference or from the knowledge or common sense of one of ordinary skill in the art.

29. I understand that for a single reference or a combination of references to render the claimed invention obvious, a POSA must have been able to arrive at the claimed invention by altering or combining the applied references.

IV. PERSON OF ORDINARY SKILL IN THE ART ("POSA")

30. I have been informed and understand that for purposes of assessing whether prior-art references disclose every element of a patent claim (thus "anticipating" the claim) and/or would have rendered the claim obvious, the patent and the prior-art references must be assessed from the perspective of a person having ordinary skill in the art ("POSA") to which the patent is related, based on the understanding of that person at the time of the patent claim's priority date. I have been informed and understand that a POSA is presumed to be aware of all pertinent prior art and the conventional wisdom in the art, and is a person of ordinary creativity. I have applied this standard throughout my declaration.

31. The '564 patent involves technology in the field of services and application implementation in communication networks. I have been asked to provide my opinions as to the state of the art in this field by early 2009. I use this timeframe because the face of the '564 patent indicates an earliest claimed priority date of January 28, 2009. Whenever I offer an opinion in this declaration about the knowledge of a POSA, the manner in which a POSA would have understood the claims of the '564 patent or its description, the manner in which a POSA would

have understood the prior art, or what a POSA would have been led to do based on the prior art, I am referencing the early 2009 timeframe, even if I do not say so specifically in each case.

32. I understand that the PO may attempt to prove that the alleged invention recited in the challenged claims was conceived at some time prior to the earliest claimed priority date on the face of the patent. At the time of this declaration, I am unaware of the PO having alleged any earlier conception date or produced any evidence to establish any earlier conception date.

33. In my opinion, a person of ordinary skill in the art in the early 2009 timeframe ("POSA") would have had (1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) 3-5 years of experience in services and application implementation in communication networks. More education could substitute for experience, and vice versa. This person would have been capable of understanding and applying the teachings of the '564 patent and the prior-art references discussed in this declaration.

34. By early 2009, I had a Ph.D. in Computer Science and Engineering and had seven years of experience in services and application implementation in communication networks beyond my Bachelor's degree, and was therefore a person of more than ordinary skill in the art. Moreover, based on my experiences, I have a good understanding of the capabilities of a POSA because I have taught,

participated in organizations with, and worked closely with many people who fit the characteristics of a POSA over the course of my career, and I am familiar with their level of skill. When developing the opinions set forth in this declaration, I assumed the perspective of a POSA, as set forth above.

V. THE '564 PATENT

A. Brief Description

35. The '564 Patent is directed to a "mobile end-user device" that includes "an inter-process software communication bus" that provides "secure communication between an executing device link agent" and "software component processes," where "software processes are allowed to access the bus based on access authorization information from a secure server that identifies those components." EX-1001, Abstract. The device link agent is configured to "maintain a secure message link" to a "message link server," over which it "receive[s] secure messages." EX-1001, Abstract.

36. In the challenged claims, "the message link server operat[es] a message service that receives messages over a network from a plurality of network functions" (Element [1D2]).[1] The "secure messages" received by the device link

[1] In this declaration, I identify limitations using the reference labels from the Claim Appendix in Section XII below.

agent are (1) "identified for delivery to multiple ones of the software components," and (2) "includ[e] message content received by the message link server from multiple ones of the network functions" (Element [1E]). "[F]or software components identified by the access authorization information," the device link agent delivers such messages to "software process[es] corresponding to the given software component[s]" over the bus (Element [1F]).

B. Prosecution History of the '403 Patent

37. The continuation application that led to the '564 Patent (application no. 15/217,538, "the '538 application") was filed July 22, 2016. The '538 application claimed priority to multiple provisional applications. EX-1001, page 2 (field (60) under "Related U.S. Application Data"). The earliest of those provisional applications was filed on January 28, 2009 ("Critical Date"). PO preliminarily amended the '538 application to replace the title and abstract and add new claims one day after the continuation application was filed, on July 23, 2016. EX-1002, 368-374.

38. The patent issued after no Office Actions. EX-1002, 531-539. TS-23.140 (EX-1004) and Rakic (EX-1007) were not cited by the Examiner, were not cited in an IDS, and do not appear in the References Cited (field (56) under "Related U.S. Application Data"). I understand that they were therefore not considered by the Examiner during the prosecution of the '564 patent.

C. Grounds for Unpatentability

39. The table below identifies each of the obviousness grounds I discuss in this declaration.

Grounds, Reference(s)		Claims	Basis
1	TS-23.140 (EX-1004), Rakic (EX-1007)	1-8, 10, 12-14	103
2A	TS-23.140, Rakic, Cole (EX-1006)	1-8, 10, 12-14	103
2B	TS-23.140, Rakic, Sathish (EX-1031)	1-8, 10, 12-14	103
2C	TS-23.140, Rakic, Cole, Sathish	1-8, 10, 12-14	103
3A	TS-23.140, Rakic, Ogawa (EX-1005)	7	103
3B	TS-23.140, Rakic, Ogawa, Cole	7	103
3C	TS-23.140, Rakic, Ogawa, Sathish	7	103
3D	TS-23.140, Rakic, Ogawa, Cole, Sathish	7	103
4A	TS-23.140, Rakic, Ellison (EX-1019)	9	103
4B	TS-23.140, Rakic, Ellison, Cole	9	103
4C	TS-23.140, Rakic, Ellison, Sathish	9	103
4D	TS-23.140, Rakic, Ellison, Cole, Sathish	9	103
5A	TS-23.140, Rakic, Shen (EX-1027)	11	103
5B	TS-23.140, Rakic, Shen, Cole	11	103
5C	TS-23.140, Rakic, Shen, Sathish	11	103
5D	TS-23.140, Rakic, Shen, Cole, Sathish	11	103

40. I am informed and understand that each reference in the Grounds qualifies as prior art to each Challenged Claim even if PO could establish entitlement to an effective filing date of January 28, 2009, on at least the bases shown below:

Reference	Filed	Published	Prior Art Basis
TS-23.140		March 2005	102(b)
Rakic	5/12/2008	11/12/2009	102(a)/102(e)
Ogawa	5/19/2008	10/1/2009	102(a)/102(e)
Cole	9/29/2006	4/3/2008	102(a)/102(e)
Sathish	10/15/2008	8/30/2011	102(a)/102(e)
Ellison	9/22/2000	7/25/2006	102(b)
Shen	3/18/2005	9/22/2005	102(b)

41. I have been asked to provide my opinion concerning whether claims 1-14 of the ’564 patent are anticipated and/or would have been obvious to a POSA in light of the prior-art references identified in the Petition. For the reasons explained below, it is my opinion that each of claims 1-14 is anticipated and/or would have been obvious to a POSA.

VI. CLAIM INTERPRETATION

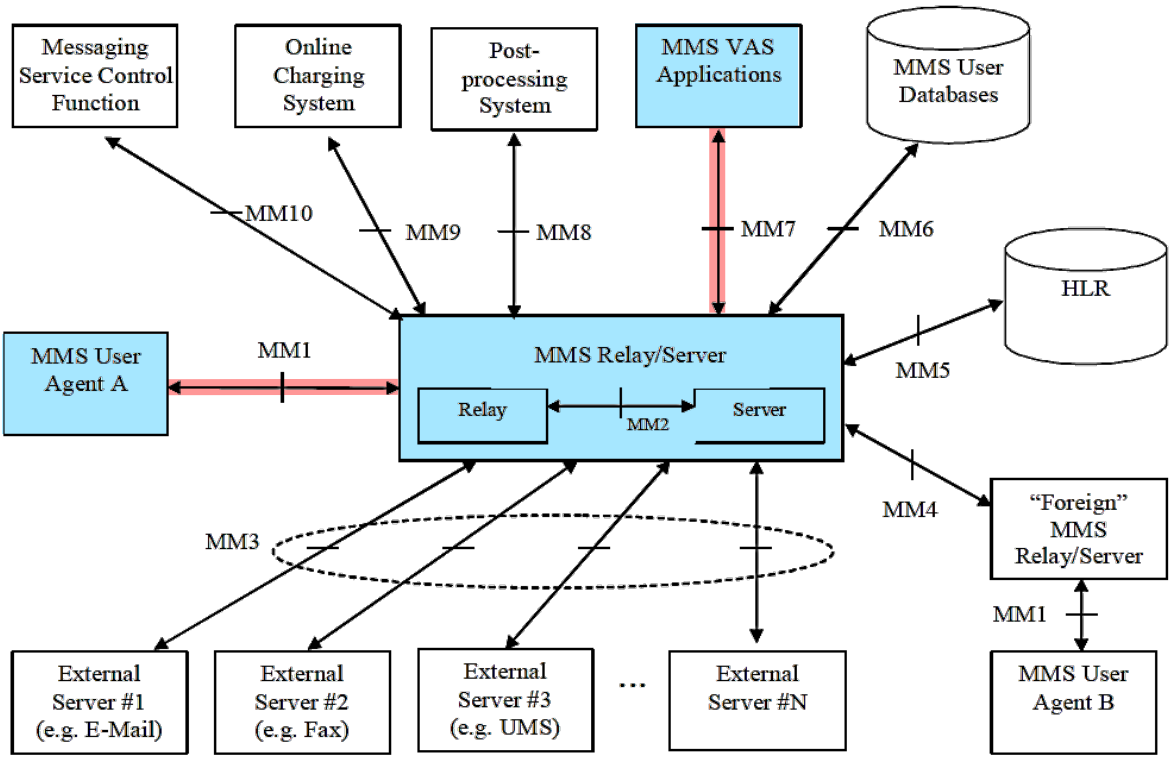
42. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent 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 as of the Critical Date (January 28, 2009). I have been informed by

Counsel that I should use the Critical Date as the point in time for claim interpretation purposes.

VII. GROUND 1: TS-23.140 AND RAKIC RENDER OBVIOUS CLAIMS 1, 3-6, AND 11-21

A. TS-23.140 (EX-1004)

43. TS-23.140 is a standard describing a "non-realtime Multimedia Messaging Service, MMS." EX-1004, 10. One MMS implementation environment is shown below, with annotations highlighting some portions of the environment:



EX-1004, 23, FIG. 3 (annotated)

44. In annotated FIG. 3 above, "MMS User Agent A" (blue box at left) is an "application residing on a UE [user equipment]… or… external device" that "performs MMS-specific operations on a user's behalf and/or on another

application's behalf." *Id.*, 14, 18-19. Those operations include, for example, retrieving multimedia messages (MMs) by "initiat[ing] MM delivery to the MMS User Agent," as well as generally "hand[ling] MMs (e.g. submitting, receiving, deleting of MMs)." EX-1004, 18-19.

45. The MMS Relay/Server (blue box in center in annotated FIG. 3 above) relays messages from the network to the MMS User Agent using interface (MM1, red). EX-1004, 17-18 (describing MMS architectural elements and FIG. 2), 21 (Section 5.2 describing MMS Relay/Server), 23-25 (Section 6 describing MMSE Architecture and Interfaces and FIGS. 3-4). The messages may include "MMS VAS" (Value Added Services) content from "MMS VAS Applications," "provided… by third-party Value Added Service Providers (VASP)" via interface MM7 (shown in red) (*id.*, 14, 18, 23), and then relayed to the MMS User Agent to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users." *Id.*, 14, 18, 23, 41. The MMS Relay/Server can relay messages from "***several*** MMS VAS Applications"[2] in the network. *Id.*, 18.

46. "MMS may… be used to transport data specific to applications" "other than the MMS User Agent…" which also "reside on [the] MMS User Agent [device]." EX-1004, 14, 54-56. I refer to the MMS User Agent "device" here in

[2] Emphasis is added throughout unless otherwise indicated.

view of the entirety of TS-23.140's disclosures—including TS-23.140's definitions of "MMS User Agent" as an "application residing on a UE, an MS or an external device…" and of "Application Data" as "[i]nformation / data specific to an application other than the MMS User Agent…" EX-1004, 14. A POSA understood that when TS-23.140 discusses transporting data specific to applications that "***reside on*** an MMS User Agent" (EX-10014, 54-56), the term "MMS User Agent" in that context refers to the client UE / MS / device.

47. The fact that the term "MMS User Agent" was sometimes used in this manner to refer to a client device with an MMS User Agent application on it is confirmed by contemporaneous references describing MMS. *E.g.*, EX-1028, 731 ("An MMS user agent (UA), also known as an MMS client, provides means for composing, sending, retrieving, viewing, and other controlling functions to users."), 732-733 (Section 2.2, describing multiple applications residing on a user device terminal implemented to use MMS for messaging). EX-1028 is a 2007 article by Mostafa, titled "Transporting data between wireless applications using a messaging system—MMS," which proposes a solution to make the enhancements in developing standards backward compatible, such that transporting application data using MMS has no impact on existing MMS services. EX-1028, Abstract. Since TS-23.140 (EX-1004) is a standard describing a non-realtime MMS and portions of the standard are expressly cited in the Mostafa reference (endnote 10),

the Mostafa reference is pertinent to the TS-23.140 standard and reflects what POSAs understood the TS-23.140 standard to teach.

48. The "application data" which may be transported to applications other than the MMS User Agent application "may be of any content type and format." EX-1004, 14. For such "application data," "the MMS User Agent… route[s] the received MMS information on to the destination application" using a "destination application identifier" included with the received message. EX-1004, 14, 56; *see generally id.,* 54-56 (Section 7.1.18, Support for transporting Application Data). "Upon reception of an abstract message containing a destination application identifier[,] the receiving MMS User Agent… shall first check if the destination application resides on [the UE device]." *Id*., 56. "If the destination application resides on a receiving MMS User Agent, the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier…." *Id*.

49. Before transporting such application-specific data, applications "register with the appropriate MMS User Agent or MMS VAS Application" by "provision[ing] an MMS User Agent or an MMS VAS Application with its application identification value and… negotiat[ing] with the MMS User Agent or MMS VAS Application the details (amount and format) of information to be exchanged between the two entities." EX-1004, 54.

50. TS-23.140 also discloses "the signing" and "encryption of an MM on an end-user to end-user basis," and using, e.g., Transport Layer Security (TLS) and "authentication mechanisms based on public/private key cryptography" for securing communications. EX-1004, 19, 41. For example, TS-23.140 notes that "[d]etails for implementation of the MM1 transfer protocol are described in Annex B." EX-1004, 25 (§6.3), 162. Annex B refers to EX-1011, which in turn refers to EX-1012 for implementation details of MM1. *See* EX-1011, 11. EX-1012 explains that "[t]he TLS [WP-TLS] transport layer security protocol provides for secure data transmission between the MMS Client and the MMS Proxy-Relay in architectural configurations that employ HTTP based protocol stacks for MMS_M implementation." EX-1012, 21. "MMS_M" is how EX-1012 refers to the "interface defined between the MMS Client and the MMS Proxy-Relay." EX-1012, 11.

B. Rakic (EX-1007)

51. Rakic discloses a system in which a "[client] device may receive" and "validate (e.g., authenticate)" "secure push message[s] based on [an] electronic signature." EX-1007, Abstract, [0039] ("validate (e.g., authenticate)"), [0050], [0044]-[0045] (describing exemplary devices), FIGS. 2A-2B (depicting a user device). "[V]alidat[ing] the secure push message[s] may protect the client device in a number of ways." EX-1007, [0041]. "For example, using the codes, the client device may authenticate the sender[,]" and/or "verify that an intended recipient of

the secure push message is the client device, and that the client device includes a correct component." EX-1007, [0041].

52. The client device "may take the form of a portable phone" or "portable digital assistant" that comprises a "[c]ommunication path" to "provide an interface through which components of [the] device… can communicate with one another[,]" and a "network interface… for communicating with other devices" "via a network," e.g., "the Internet," "a WLAN," and "UMTS [(i.e., 3G)]." EX-1007, [0001], [0013] (the user device may be a "cell phone"), [0051]-[0052] (describing the components of the user device), [0057] (describing the user device's network interface), [0122], FIGS. 2A-2B. The client device also comprises a "[d]isplay [that] may provide visual information to the user" and "[c]ontrol buttons [that] permit the user to interact with [the] client device[.]" EX-1007, [0052]. The client device "may include additional functional components, such as… an application (e.g., an instant messenger client…)" (EX-1007, [0059]) and "may perform a specific task" "related to an application" "in accordance with contents of [a] secure push message" (EX-1007, [0051]).

53. Rakic further discloses an "administrator device," which "may include… a secure push message server" and "additional functional components, such as… an application (e.g., an email server, a[] file transfer protocol (FTP) server, etc.)" EX-1007, [0045], [0063] (describing Figure 5 and certain

components of the administrator device). The "[s]ecure push message server… may send secure push messages to client device… via a wireless network[.]" EX-1007, [0065]. The administrator device "may include a database of information about client device[s]." EX-1007, [0047], [0069] ("database 602 may be included in administrator device 104" and "may be used to create keys for generating electronic signatures").

54. Rakic discloses that "[g]iven a message or a payload from an application… secure push message server… may generate a key, an electronic signature, and a secure push message." EX-1007, [0065]. The key may be generated by creating a hash of an administrator code and identifying information for a client device (or component thereof). EX-1007, [0042] ("The format of the secure push message… may be easily modified to accommodate different types of applications/devices that receive/send secure push messages"), [0066]-[0068], [0071]-[0072] (the "record [for a client device (or component thereof)] may include additional, fewer, or different fields than those illustrated in FIG. 7"), [0080], [0085] ("push message server… may automatically generate the administrator code."). A POSA thus understood that the key may be generated by creating a hash of an administrator code generated by the push message server and the identifier of a component (e.g., an application) of a client device. Administrator device and client device may exchange the administrator code and identifying

information for a client device (or component thereof) during initial configuration. EX-1007, [0048].

55. "Once the key is generated, secure push message server… may generate an electronic signature based on the key and the message" by "signing [the] message with [the] key." EX-1007, [0066], [0040], [0049] (discussing generation of a key and signing of a message), [0080] (providing a key generation expression), [0105] (describing the key generation and message signing process). The "secure push message server… generate[s] the secure push message by appending the electronic signature to the message[.]" EX-1007, [0067], [0079] (providing a signature generation expression). A POSA would have been familiar with standard cryptographic algorithms used to create the key and the signature, including hash functions (e.g., SHA-256) and message authentication code (MAC) algorithms (e.g., HMAC-SHA256).

56. Figure 8 depicts a secure push message, comprising the push message (blue) and the signature (green):

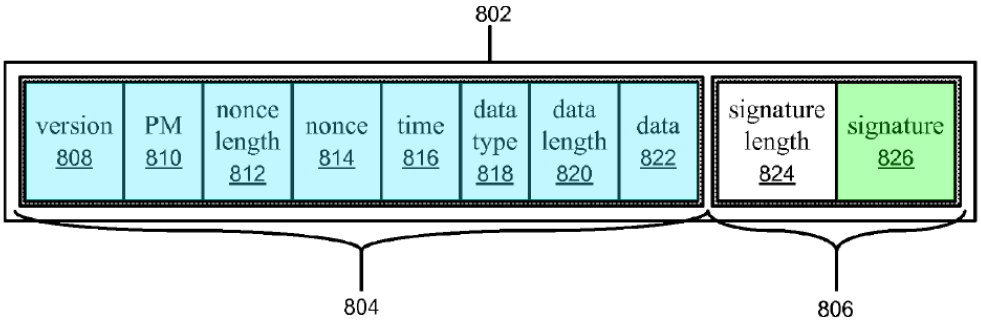


Fig. 8

EX-1007, FIG. 8. The message body further comprises "[d]ata field 822[, which] may include content (e.g., payload)[,]" and "PM field 810[, which] may indicate a particular method that is used to generate a signature, to encrypt the data, or ***to perform a combination of generating a signature and encrypting the data***." EX-1007, [0075], [0078].

57. Secure push server then sends the secure push message to the client device, which secure push message client of client device attempts to "validate… based on the electronic signature." EX-1007, [0050], [0040] (discussing secure push message validation), [0065] ("secure push message server 504 may generate a key, an electronic signature, and a secure push message."). To do so, the secure push message client first constructs the key in the same manner as the secure push server—by creating a hash of the administrator code and the identifying information for the client device (or component thereof). EX-1007, [0110]-[0111] (describing the client device's process of generating a key). The secure push

message client then signs the data block of the received message with the key and compares the result to the signature of the received message. EX-1007, [0112] (describing the client device's process of generating a signature). If the signatures match, the secure push message client determines that the message is valid. *Id.* If the message is valid and the data block contains data intended for a "component[of the client device], such as… an application[,]" the data is sent to the component. EX-1007, [0112]-[0119] (explaining that processing of the push message continues only if it is deemed valid by the secure push message client), [0122] (explaining that the data can cause a component to perform a task), [0130]-[0131] (providing example of the data causing a component to perform a task).

C. The MMS-Rakic Combination

58. As discussed below, "MMS-Rakic" refers to an encrypted MMS system in which communications with the MMS User Agent on TS-23.140's user device—which may occur over a network (e.g., with an MMS Relay/Server) or within the device (e.g., with other applications)—are secured using Rakic's message signing and validation teachings.

1. Implementing TS-23.140's User Device with a Modem

59. As I noted above (*e.g.*, in Section VII.A, paragraphs 44, 46), TS-23.140 says its "MMS User Agent" "resid[es] on a UE [user equipment]… or… external device." EX-1004, 14, 18-19. TS-23.140 describes the User Agent as

communicating with the MMS Relay/Server using, e.g., "2G and 3G wireless networks," but does not disclose details regarding how the device on which the User Agent resides facilitates communications over such networks. *E.g.,* EX-1004, 17, 23-24, FIG. 2 (annotated below).

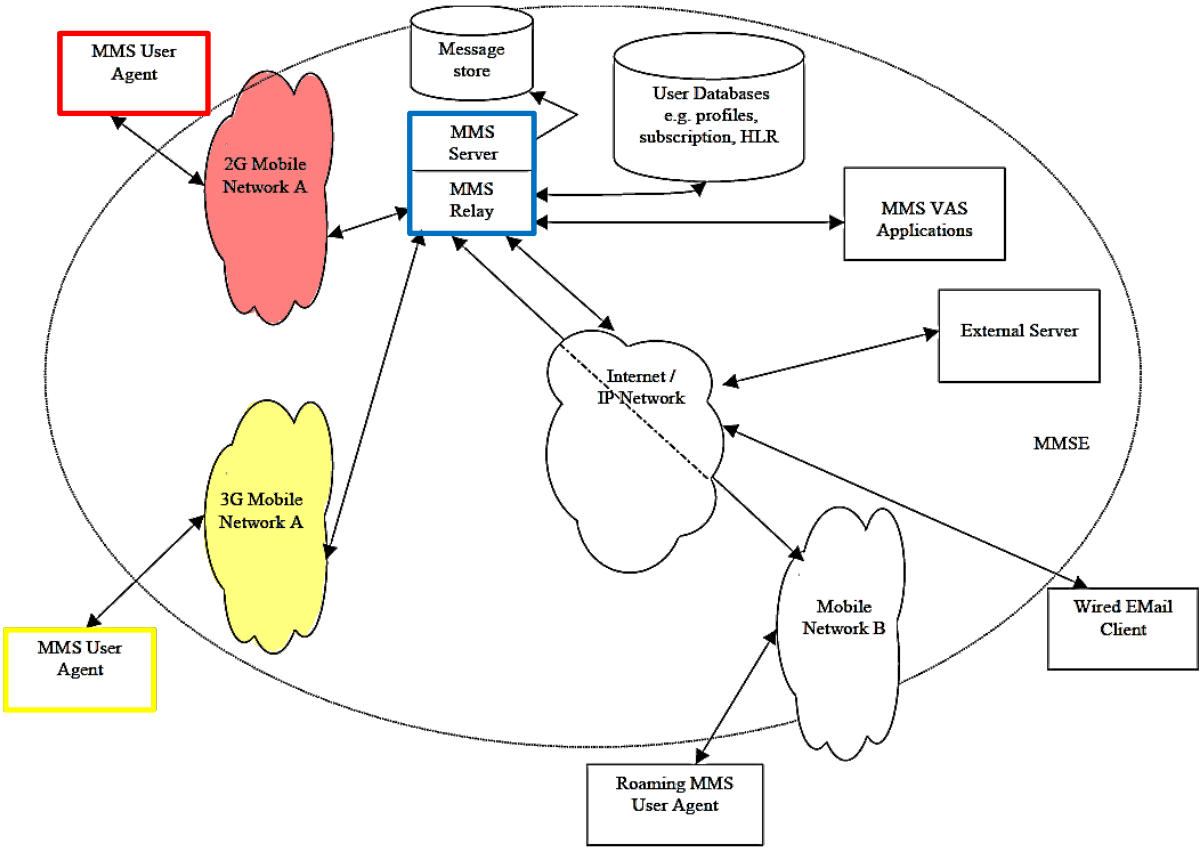
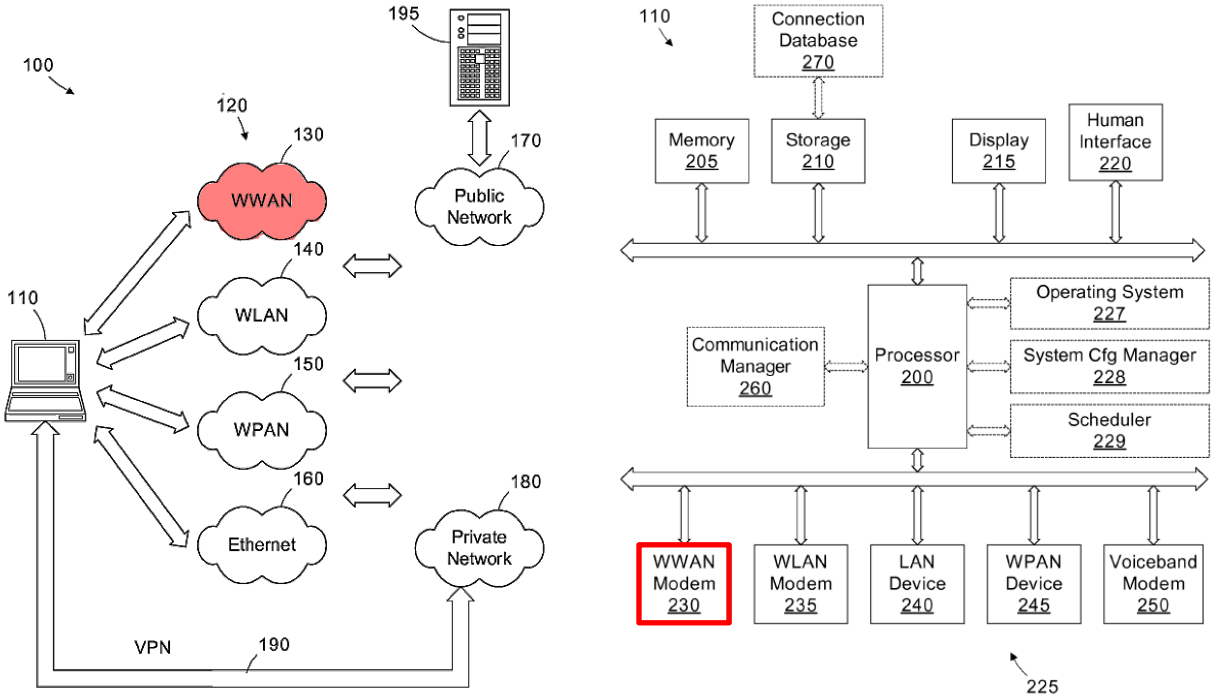


Figure 2: MMS Architectural Elements

EX-1004, FIG. 2 (annotated)

60. Before the Critical Date, it was well-known and well-documented to use a ***modem*** to enable communications over the networks described in TS-23.140, and a POSA would have been motivated to do so. For example, Cole (EX-1006)

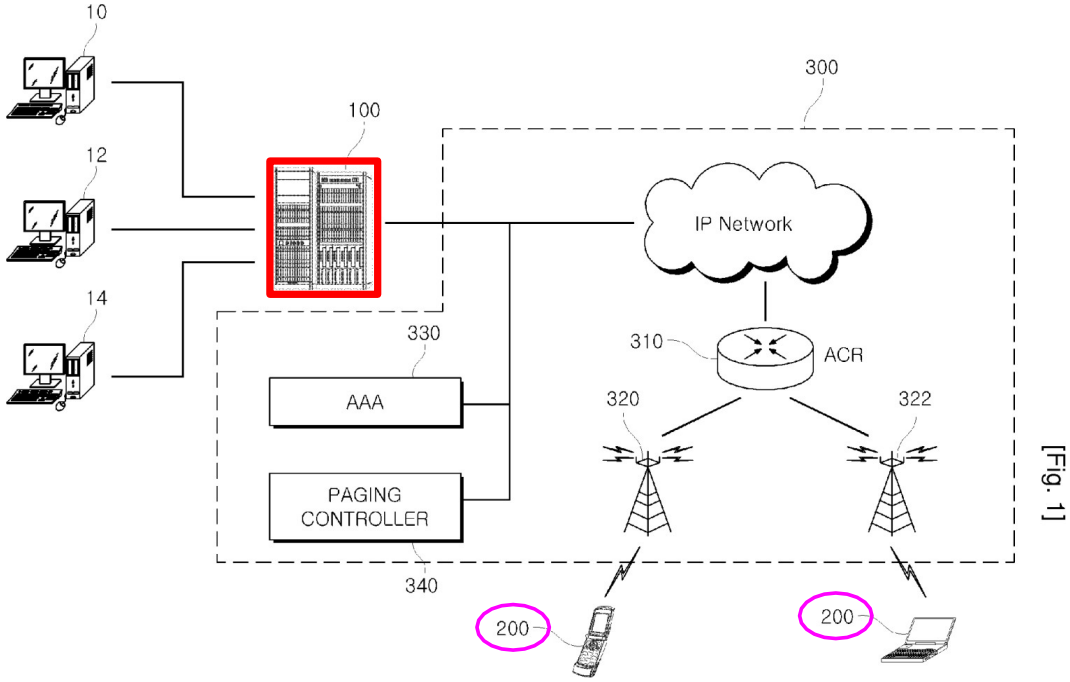
discloses a modem for connecting a client (Cole's "mobile device") to a server through a 2G or 3G network. *See* EX-1006, [0003], [0031]-[0035] ("The communication system 100 includes a mobile device 110 interfacing with a plurality of communication networks 120, such as a wireless wide area network (WWAN) 130 (e.g., … {3G} cellular technologies, … {2G} cellular technologies) … Exemplary communication interfaces 225 that may be provided include a WWAN modem 230, a WLAN modem 235, a LAN device 240, a WPAN device 245, and a voice band modem 250 (e.g., V90)."); FIG. 2 (below).



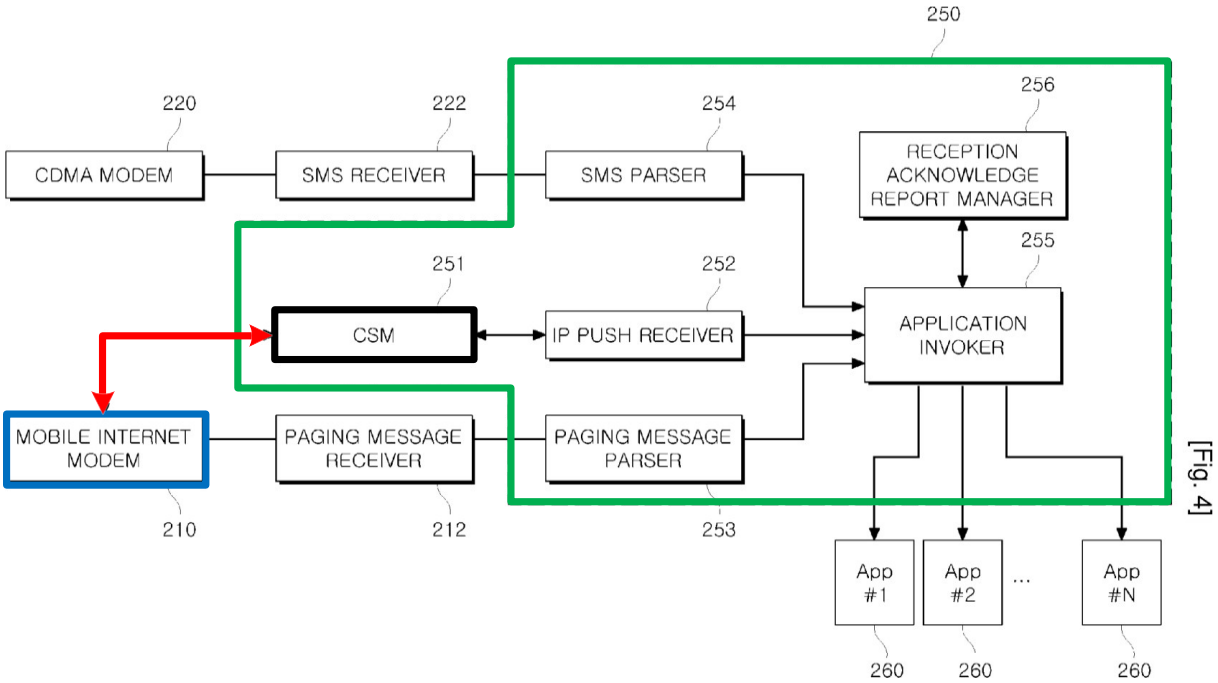
EX-1006, FIGS. 1-2 (annotated)

61. Another example is Lee (EX-1008), which is a corroborating reference in the general technical field of push communications between network

entities and applications executing of a user device. Lee (EX-1008), Abstract, ¶¶ 1, 8, 27-28, 44, FIGS. 1, 4. Like the MMS User Agent on the user device in TS-23.140 that receives messages from MMS relay/server, in Lee, a service agent 250 (green in FIG. 4 below) on mobile terminal 200 (pink) receives messages from a service server 100 (red), and the mobile terminal 200 receives the messages through a mobile internet modem 210 (blue). EX-1008, ¶¶ 22-23, 27-28.



EX-1008, FIG. 1 (annotated)



EX-1008, FIG. 4 (annotated)

62. Using a modem to enable a user device to communicate over the wireless networks in TS-23.140 would have been a conventional, obvious way to implement what TS-23.140 describes, and is nothing more than using familiar, known components to achieve a predictable result of facilitating TS-23.140's communications. Indeed, a POSA would have found it obvious for a computing device to use known networking components, such as a modem, to achieve the predictable result of facilitating network communications, as already contemplated by TS-23.140. Thus, in view of TS-23.140's teachings of network communication between user devices and networked servers (which I discussed in, *e.g.*, paragraphs 44-45 above), and knowledge of a POSA before the Critical Date (as evidenced by Cole's (EX-1006) and Lee's (EX-1008) disclosures of the user device using a

modem to facilitate such network communications, as I discussed in, *e.g.* paragraphs 60-61 above), a POSA would have found it obvious to implement TS-23.140's system to include a ***modem*** to facilitate the above-described network communications. A POSA would have reasonably expected success in implementing TS-23.140's device with a modem because this was a well-known, conventional way (*e.g.,* EX-1006, [0031]-[0035]; EX-1008, ¶¶22-23, 27-28) of achieving the wireless network communications that TS-23.140 describes (*e.g.,* EX-1004, 17, 23-24, FIGS. 2-4).

63. In IPR2024-00341, the Board agreed, "find[ing] that the cited portions of the record show that modems were known for enabling communication over networks, such as those described in TS-23.140" and "credit[ing] Petitioner's testimonial evidence regarding modems and that one of ordinary skill would have implemented TS-23.140 to include a modem with a reasonable expectation of success because the cited portions of the record support the testimony." EX-1022, 40-41 (citing, e.g., EX-1004, 14, 17-19, 23-24; EX-1008, ¶¶27-28, 44, FIGS. 1, 4).

2. Securing Interface MM1 Using SSL/TLS

64. TS-23.140 explains that network communications between the MMS User Agent and the MMS Relay/Server use interface MM1. EX-1004, 24, FIG. 4 (below).

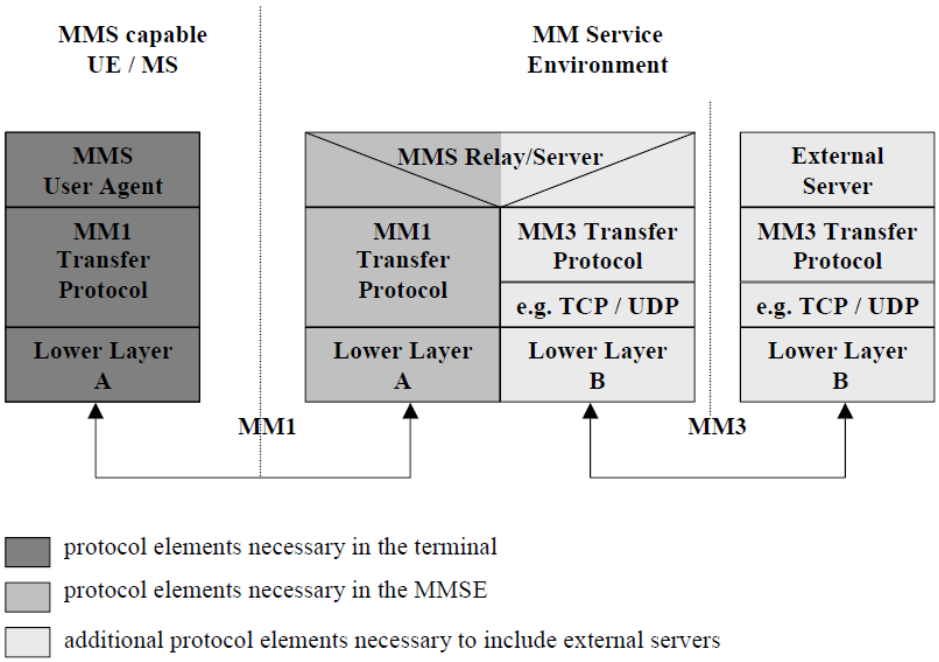


Figure 4: Protocol Framework to provide MMS

EX-1004, 24, FIG. 4

As shown in the figure above, the MM1 Transfer Protocol for the MM1 interface is implemented both at the MMS Relay/Server and the MMS UE. *See* EX-1004, 24, FIG. 4. A POSA would have understood that the MM1 interface which uses the MM1 Transfer Protocol facilitates transmission/transport of network communications between the MMS User Agent and MMS Relay/Server (and with other network elements via the MMS Relay/Server, such as MMS VAS Applications, which additionally leverage the MM7 transport interface). *See also*, *e.g.*, EX-1018, 6 (MM1 Interface is an "[i]nterface between MMS Relay/Server and MMS User Agent"; MM7 is "[i]nterface between MMS Relay/Server and MMS VAS Applications"), 9 (FIG. 1 showing MMS architecture including MM1and MM7 interfaces).

65. A POSA had multiple reasons to secure interface MM1 with an SSL/TLS protocol, as I explain below.

66. ***First,*** TS-23.140 expressly contemplates implementations which use "transport layer security mechanisms" (e.g., SSL/TLS) to secure its communication links, including MM1 between the user device (with the MMS User Agent) and the MMS Relay/Server. For example, TS-23.140 teaches an "WAP/OMA implementation" for the MM1 interface between the MMS User Agent (on the user device) and the MMS Relay/Server. EX-1004, 30, 55, 162, 174. WAP/OMA refers to Open Mobile Alliance's "Wireless Application Protocol." EX-1004, 13 (citing numerous "Open Mobile Alliance" references), 16 (defining WAP acronym). To describe "[d]etails" for this "implementation of the MM1 transfer protocol," TS-23.140 incorporates-by-reference EX-1011, an "Enabler Release Definition." *See* EX-1004, 13, 24-25, 162. EX-1011, in turn, incorporates-by-reference EX-1012, an "Architecture Overview." EX-1011, 4, 5, 10, 11. The Architecture Overview states that "[t]he ***TLS*** [WP-TLS] transport layer security protocol ***provides for secure data transmission between the MMS Client and the MMS Proxy-Relay*** in architectural configurations that employ HTTP based protocol stacks for MMS_M implementation." EX-1012, 21. In TS-23.140's disclosed WAP/OMA implementation of MMS, the "MMS User Agent is… responsible for sending and receiving MMs by utilising the message transfer

services of the appropriate network protocols," e.g. SSL/TLS for securing MM1 between the MMS User Agent and the MMS Relay/Server. EX-1012, 17, 21. TS-23.140 includes similar disclosures regarding other communications links, e.g. MM7 between the MMS Relay/Server and the MMS VAS Applications. *E.g.,* EX-1004, 41 ("interface [MM7] between MMS Relay/server and VASP may be carried over an encrypted and secure bearer, e.g. HTTP over SSL or TLS[.]").

67. ***Second,*** it was well-known and well-documented before the Critical Date to use SSL/TLS to achieve secure communications between entities on a network, e.g. between a client and server. *See*, *e.g.*, EX-1012, 21 (disclosing "encrypt[ing]" the communication channel between the client and the backend MMS server with some security protocols, e.g., WTLS (Wireless Transport Layer Security)); EX-1010, 1:38-42 ("A variety of ***cryptographic techniques*** are known for securing transactions in data networks. ***For example, the Secure Socket layer (SSL) protocol and its successor Transport Layer Security (TLS) provides a mechanism for securely sending data between a server and a client***."); EX-1013, 3 ("Cryptographic security[:] SSL should be used to establish a secure connection between two parties.").

68. ***Third,*** such an implementation is nothing more than using familiar, known protocols to achieve a predictable result of facilitating secure communications with TS-23.140's User Agent over MM1.

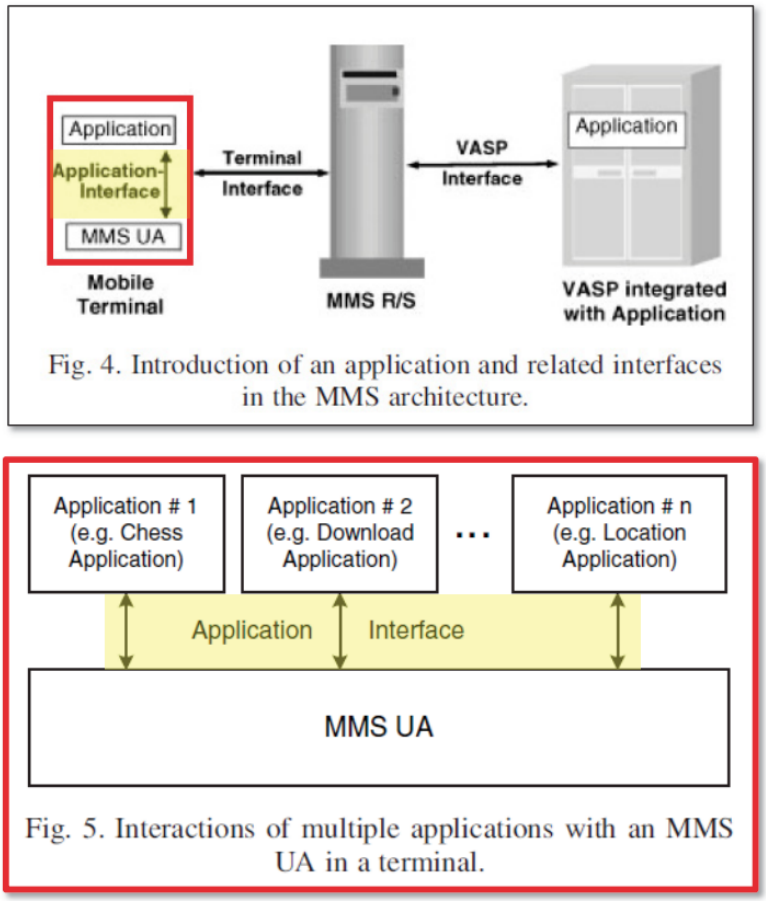
69. A POSA would have reasonably expected success implementing MM1 to use SSL/TLS, given TS-23.140's teachings and incorporated disclosures, and the widespread use of such security protocols before the Critical Date.

70. In IPR2024-00341, the Board agreed, "find[ing] that the cited portions of the record support that one of ordinary skill in the art would have used SSL/TLS protocol" for MM1, "and that such use would have had a reasonable expectation of success," and "credit[ing] Petitioner's testimonial evidence" regarding same "because the record supports it." EX-1022, 41-42 (citing, e.g., EX-1004, 24-25, 55, FIG. 4; EX-1010, 1:38-42; EX-1012, 21; EX-1013, 3; EX-1018).

3. Implementing TS-23.140's User Device with an Interprocess Communication Bus

71. TS-23.140 discloses its MMS User Agent receiving "data specific to an application other than the MMS User Agent" from MMS VAS Applications and "rout[ing]" that "received MMS information" (such as application-specific data) "to [a] destination application" on the user device—but leaves it to a POSA the "[d]etails of… how an MMS User Agent… would ***interface*** with" the user device's destination applications. EX-1004, 54-56 (Section 7.1.18; Support for transporting Application Data). Contemporaneous references discussing MMS confirm that TS-23.140's UE included an interface for communications between the MMS User Agent and other applications. *E.g.*, EX-1028, 729-730 (discussing the "interface between an application and MMS in a terminal"), 732-733

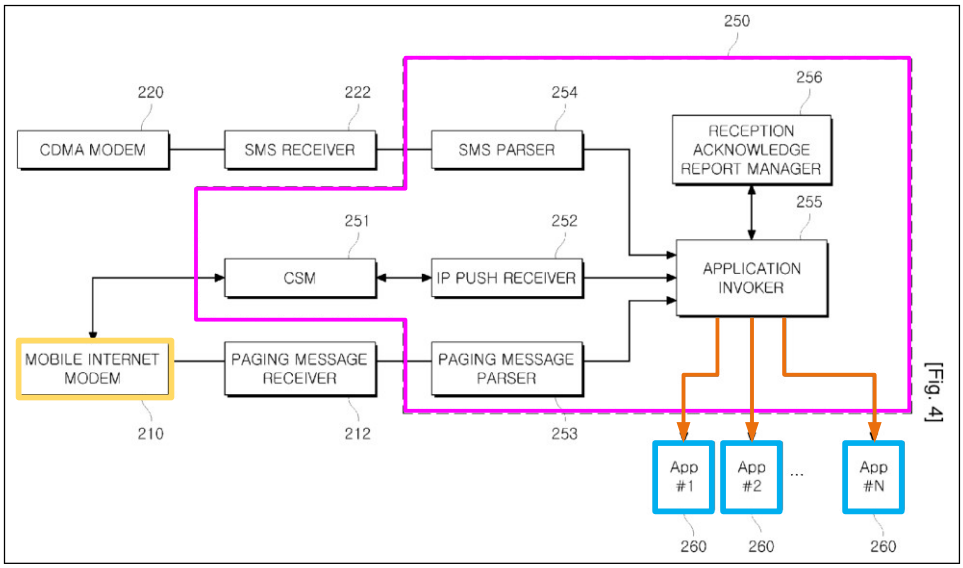
(discussing the "application-interface between an application and an MMS UA" "within an MMS-capable terminal"), FIGS. 4-5 (annotated below).



EX-1028, FIGS. 4-5 (annotated)

72. As another example, Rakic confirms the presence of such "communication path[s]" in the context of devices that receive push messages from servers. Rakic discloses a "[c]ommunication path 310" that "provide[s] an interface through which [device] components… communicate with one another." EX-1007, [0058], FIG. 3. Rakic discloses that the device components interfacing through communication path 310 include "application[s, such as] an instant messenger client[.]" EX-1007, [0059].

73. As another example, Lee (EX-1008) corroborates that there would be a communication channel in the end-user device between a push service agent 250 that receives messages intended for applications resident on a device from external sources, and a target application 260 to which the service agent 250 sends the message. EX-1008, ¶28. As shown in Lee's FIG. 4 below, the push service agent 250 (***device link agent***) is ***communicatively coupled*** to the multiple applications 260 (***the plurality of software components***) ***through a communication bus*** including respective communication channels (depicted in orange in figure below).



EX-1008, FIG. 4 (annotated)

74. A POSA would have had reason to (and would have been motivated to) implement the interface between TS-23.140's MMS User Agent application and the user device's other applications using a software ***bus*** for interprocess communications—for example, a D-bus. Before the Critical Date, it was well-known and well-documented to use a software bus (e.g., a D-bus) for inter-process

communications that enable applications to interface with one another, as TS-23.140 describes. *See, e.g.*, EX-1031, 10:56-62 ("[T]he D-Bus may be an example of a device inter-process communication channel used to send information between applications. As such, method calls made over the D-Bus may be serialized as a message addressed to a particular application. The particular application may then listen and perform the service requested and place an output back on the D-Bus addressed to the browser application."); EX-1048, [0001], [0003], [0004], [0019] (describing "communication" between "one or more processes" occurring over a "bus"); EX-1049, 907 (defining "software bus": "A programming interface that allows software modules to transfer data to each other…."); EX-1050, 2:64-3:6 (describing "software bus" that "interconnects" a "control software's subsystems"), 3:51-67, FIG. 5.

75. Using such a bus to enable an MMS User Agent to communicate with other applications on TS-23.140's user device would have been a conventional, obvious way to implement what TS-23.140 describes, and is nothing more than using familiar, known components (as I discussed in paragraphs 71-74 above) to achieve a predictable result of facilitating TS-23.140's communications.

76. Moreover, a POSA would have reasonably expected success with such an implementation because a software bus (e.g., a D-bus) was a well-known, conventional way of achieving the communications between applications that TS-

23.140 describes (as evidenced by, for example, the references I discussed in paragraphs 71-74 above).

77. In IPR2024-00341, the Board agreed with Petitioner that the implementation I discussed above in this Section would have been obvious. In response to Petitioner's "argu[ment] that [a POSA] would have implemented communications between the MMS User Agent and other applications over a bus, such as a D-bus" (EX-1022, 45), the Board found that a POSA "would have implemented a bus for communications between the destination applications and the MMS User Agent[,]" "credit[ing] Petitioner's testimonial evidence that a bus was known for inter-process communication and would have been a conventional way to implement what TS-23.140 describes, because the cited portions of the record support it… [and] that using such a bus would have been using a known component to achieve the predictable result of providing the described communications between the MMS User Agent and destination applications." EX-1022, 48 (citing, e.g., EX-1008, [28], FIG. 4; EX-1028, 732-733; EX-1031, 10:56-62). The Board "also credit[ed] the testimony that the implementation would have had a reasonable expectation of success." EX-1022, 48-49.

4. Applying Rakic's Message Validation Techniques

78. TS 23.140 discloses "[t]he MMS User Agent… provid[ing] additional application layer functionalities such as... the ***signing*** of an MM on an end-user to

end-user basis[,]" but does not provide details regarding how to implement such signing functionality between network entities. EX-1004, 19, 54-56 (Section 7.1.18; Support for transporting Application Data).

79. As I discussed in Section VII.B above, Rakic discloses details regarding how to implement digital signatures in messages sent by a secure push message server to a client device. EX-1007, Abstract, [0041], [0044]-[0045], [0050]. Rakic discloses a system for "validat[ing]… secure push message[s] based on [an] electronic signature[,]" which is created by "sign[ing] a data block within the secure push message" with a key. EX-1007, Abstract, [0041], [0050]. The validation is performed to "authenticate the sender" of a message and/or "verify that an intended recipient of the secure push message is the client device, and that the client device includes a correct component." EX-1007, [0041].

80. A POSA had multiple reasons to implement Rakic's message signing and validation techniques for messages containing content sent by an MMS VAS Application to an MMS User Agent, as I explain below:

81. ***First***, TS-23.140 expressly teaches having the MMS User Agent handle signing of MMs on an end-user to end-user basis, and Rakic (as I discussed above in Section VII.B) provides details regarding how to implement the signature functionality that TS-23.140 discloses. EX-1004, 19; *e.g.,* EX-1007, Abstract,

[0041], [0050], [0079]-[0080] (describing the key and signature generation process), [0104]-[0105] (describing similar).

82. ***Second***, a POSA would have understood that implementing Rakic's validation process on TS-23.140's MMS User Agents for messages containing signed content originating from MMS VAS Applications would enhance the reliability and security of TS-23.140's MMS system by ensuring that messages routed to destination applications originated from an authorized source, that the routing information has not been tampered with, and that only the intended destination application (the application identified by TS-23.140's destination application identifier) receives it. EX-1007, Abstract, [0041] ("For example, using the codes, the client device may authenticate the sender. In another example, using the codes may verify that an intended recipient of the secure push message is the client device, and that the client device includes a correct component."), [0042] ("The format of the secure push message… may be easily modified to accommodate different types of applications/devices that receive/send secure push messages."), [0050] ("client device 102 may validate the secure push message based on the electronic signature"), [0059] (disclosing that the client device "component" may be an "application"), [0070]-[0071] (disclosing use of "additional… or different fields than those illustrated in FIG. 7"—e.g., as a POSA

understood, for identifying the "correct component" per my discussion below in paragraph 117).

83. ***Third***, implementing Rakic's signature-generation and verification process into TS 23.140's MMS system would have been nothing more than applying known message signing and validation techniques (e.g., signature verification) to known components (MMS VAS Application and MMS User Agent) to achieve predictable results (end-user-to-end-user message delivery in which the MMS User Agent verifies that received, signed messages are from a valid source).

84. A POSA would have reasonably expected success implementing Rakic's message validation techniques to the TS-23.140 system given (1) TS-23.140 and Rakic share a similar push-message architecture, in which a network server transmits content to a client device; and (2) TS-23.140 contemplates MMS User Agents signing MMs on an end-user-to-end-user basis, and Rakic provided an exemplary, predictable implementation of such message validation using signature-generation and verification. A POSA further understood that TS 23.140's disclosure of "signing MMs on an end-user-to-end-user basis" was also applicable to MMS VAS Applications. EX-1004, 23 ("The MMS VAS Applications provide value added services to the MMS users. ***In many ways MMS VAS Applications behave like a fixed MMS User Agent.*** However, MMS VAS Applications may

provide some additional features like MM recall between MMS VAS Applications and MMS Relay/Server which are not available for MMS User Agents.”).

85. In such an implementation, a POSA would have incorporated the secure push message signing functionality of Rakic’s secure push message server into TS-23.140’s MMS VAS Application, and would have incorporated the signature validation functionality of Rakic’s secure push message client into TS-23.140’s MMS User Agent. I described Rakic’s secure push message signing functionality and signature validation functionality in Section VII.B above.

86. Additionally, during the application registration process described in TS-23.140—where an application “provisions an MMS User Agent or an MMS VAS Application with its application identification value and… negotiates with the MMS User Agent or MMS VAS Application the details (amount and format) of information to be exchanged between the two entities” (EX-1004, 54)—the necessary information used to create keys for signing and signature validation (e.g., the VAS Application’s administrator code) are provisioned as needed to facilitate Rakic’s message signing and signature validation functionality. EX-1004, 54-56; EX-1007, [0048] (“During the configuration, administrator device 104 may obtain ***information that is specific to client device 102***,… and ***store an administrator code in client device 102***.”). A POSA would have understood that after the provisioning process, both MMS-Rakic’s VAS Application and User

Agent would have the needed information—e.g., the VAS Application's administrator code and the destination application's identification value—to generate the key used to sign and verify MMs.

5. MMS-Rakic

87. "MMS-Rakic" refers to the above-discussed encrypted MMS system that a POSA would have been led to form based on TS-23.140 and Rakic.

88. MMS-Rakic implements TS-23.140's user device (configured to use TS-23.140's MMS service) with a modem for wireless network communications. *See* my discussion above in Section VII.C.1, at paragraphs 59-63.

89. MMS-Rakic also implements TS-23.140's MMS Relay/Server and user device so that messages transmitted across the interface between TS-23.140's user device and the MMS Relay/Server are secured with SSL/TLS. *See* my discussion above in Sections VII.C.2, at paragraphs 64-70.

90. MMS-Rakic also implements an interprocess bus for communications that occur within TS-23.140's user device between applications (*see* my discussion above in Section VII.C.3, paragraphs 71-77).

91. Additionally, in MMS-Rakic, Rakic's secure push message signing functionality is implemented as part of TS-23.140's VAS Application, and Rakic's signature validation functionality is implemented as part of TS-23.140's MMS

User Agent in a user device (*see* my discussion above in Section VII.C.4, paragraphs 78-86).

D. Claim Analysis

1. Claim 1

a. [1PRE] A mobile end-user device comprising:

92. The ’564 specification[3] does not describe a “mobile end-user device,” but uses the term “end user device.” *See*, *e.g.*, EX-1001, 7:53-65, 8:44-67. The ’564 specification defines no requirements for an “end user device.” *See, e.g.*, EX-1001, 8:3-15, 8:60-9:15, including generic descriptions of devices). It instead uses the term to include “networked” devices that have “services delivered” to them. EX-1001, 5:41-6:8 (“connected (e.g., networked)” devices), 6:30-38 (“service” functions, consumption, costs). A POSA understood that the “devices” described in columns 5-6 were the “end user devices” described in columns 7-8. A POSA understood TS-23.140’s “UE,” “MS,” “external device,” and “mobile phone” to be examples of subscriber wireless devices, such as the specification describes (EX-1001, 5:41-6:8). In addition, in IPR2024-00341, the Board found “that the User

[3] When I refer to “the ’564 specification” in this declaration, I refer to EX-1001, 1:1-168:62 and FIGs. 1-64, which reflect the disclosure that was included in the July 22, 2016 continuation application. EX-1002, 121-361. This does not include the title or abstract, which were added later, on July 23, 2016. EX-1002, 369.

Equipment of TS-23.140 teaches, suggests, or would have been understood to disclose, to the extent the preamble is limiting, '[a]n end-user device.'" EX-1022, 15.

93. A POSA would have understood MMS-Rakic's "UE [***user*** equipment]"/"MS"/"external ***device***"/"***mobile*** phone"—with an MMS User Agent that "performs… operations on a ***user's*** behalf," through which "Value Added Services" are "provided" (delivered) to "***users***"—is a "***mobile*** end-user device." EX-1004, 14 (MMS User Agent), 18, 54.

b. [1A] a wireless modem configurable to exchange data via a connection to a wireless network;

94. As I discussed above in Section VII.C.1, MMS-Rakic includes a "***modem***." In IPR2024-00341, the Board credited Petitioner's showing of "a modem" for network communications because "TS-23.140 shows an MMS User Agent communicating through interface MM1 with an MMS Relay/Server, MMS VAS Applications, MMS User Databases, and other components," and "[t]he other-relied upon portions describe those components and sending and receiving messages between an MMS User Agent or MMS VAS Application and a destination application over wireless networks." EX-1022, 15-16 (citing EX-1004, 14, 18, 23-25, 55-56, FIGs. 2-4).

95. Element [1A] requires "a ***wireless*** modem." MMS-Rakic's modem is for communications over 2G and 3G wireless networks (see my discussion above in Section VII.C.1) and is thus "a ***wireless*** modem," as claimed.

96. A POSA further understood that MMS-Rakic's modem for 2G and 3G wireless networks (see my discussion above in Section VII.C.1) is also "configurable to exchange data via a connection to a wireless network," as claimed. This is confirmed, for example, in FIG. 2 of TS-23.140, which shows an exemplary Multimedia Messaging Service Environment (MMSE) in which TS-23.140's user device (MMS-Rakic's user device—see my discussion above in Section VII.D.1.a, discussing [1PRE])) operates, comprising 2G (red) and 3G (yellow) wireless networks:

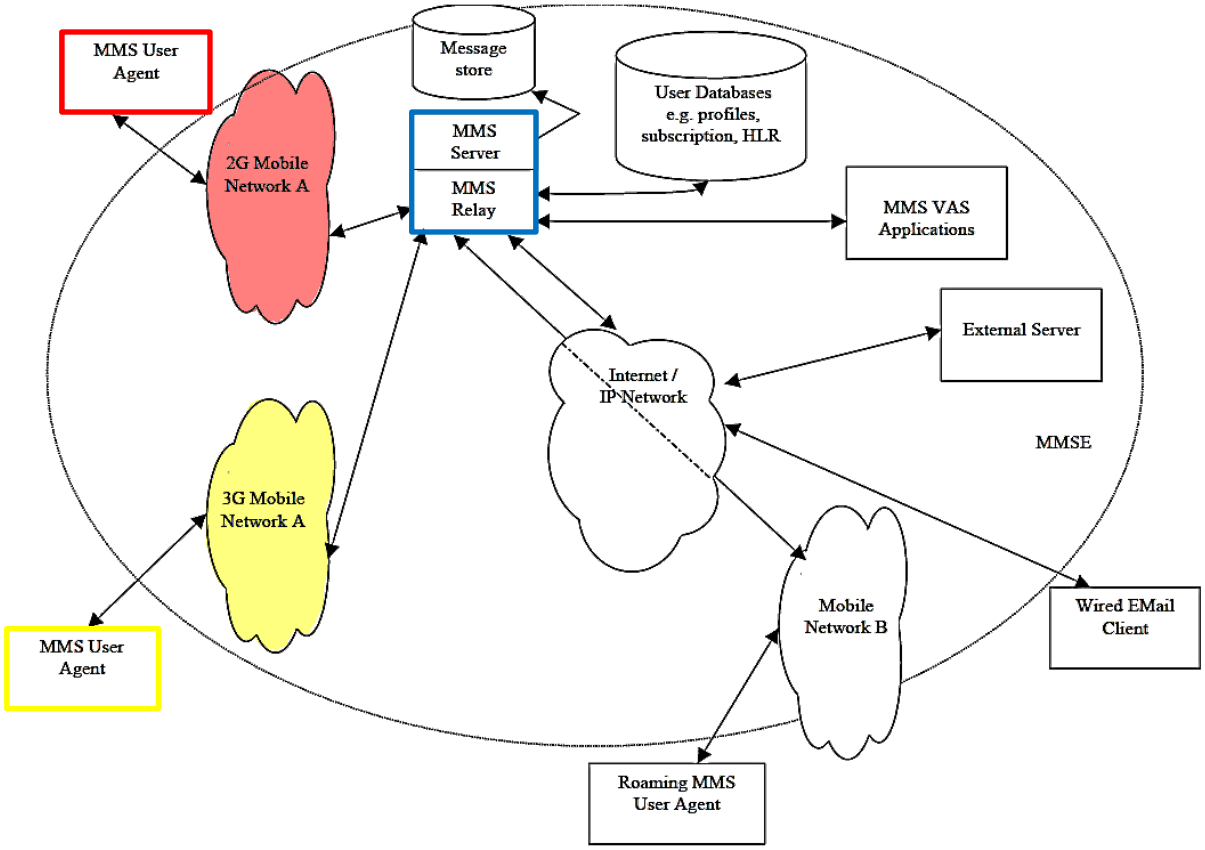
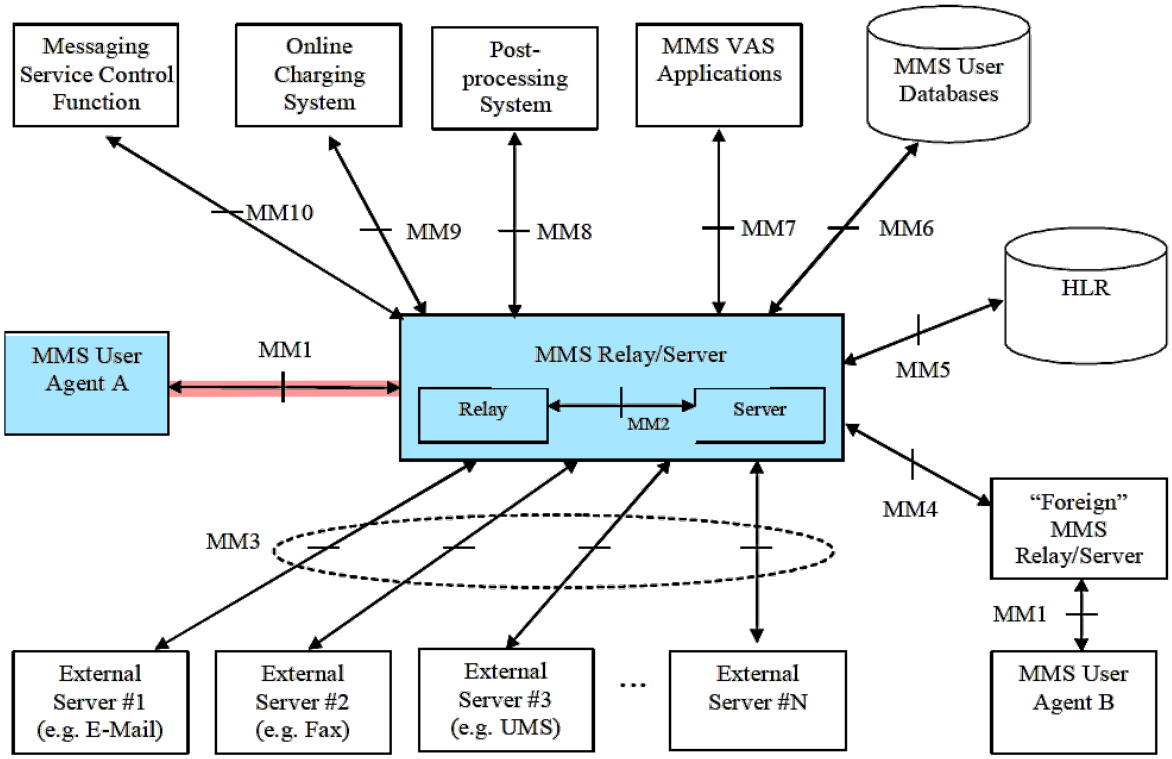


Figure 2: MMS Architectural Elements

EX-1004, 17, FIG. 2 (annotated)

97. Above, multiple "MMS User Agent" UEs are illustrated—including one (top left) that is configured for communications with the MMS Relay/Server through a connection to "2G Mobile Network A," and another (bottom left) that is configured for communications with the MMS Relay/Server through a connection to "3G Mobile Network A." EX-1004, 14, 17-19, 23-24 (each discussing 2G and 3G). A POSA understood these connections are part of the respective interface MM1 for each user device which facilitates the wireless communications between each user device's MMS User Agent and the MMS Relay/Server. EX-1004, 17,

23-24, FIG. 4 (Protocol Framework to provide MMS). Interface MM1 is annotated red in FIG. 3 below:



EX-1004, 23, FIG. 3 (annotated)

98. The modem in MMS-Rakic's user device also enables MMS-Rakic's User Agent to exchange messages containing ***data*** with network elements through interface MM1—including with MMS-Rakic's Relay/Server, and multiple VAS applications (via the Relay/Server). EX-1004, 14 (definition of application data), 18 (4.3 describing addressing for messages), 23-24 (depicting/describing FIG. 3). For example, using the modem, MMS-Rakic's User Agent may "transport ***data*** specific to applications other than MMS" (e.g., in "abstract messages") to or from

a VAS Application. EX-1004, 17 (FIG. 2, showing/describing MMS architectural elements), 54-56 (Section 7.1.18, Support for transporting Application Data).

99. Thus, a POSA understood that MMS-Rakic's modem (see my discussion above in Section VII.C.1) is "configurable to exchange ***data*** via a connection to" MMS-Rakic's wireless networks.

c. [1B1] an inter-process software communication bus providing secure communication between an executing device link agent and respective executing processes for a plurality of software components,

100. MMS-Rakic meets each limitation in Element [1B1], as I discuss below.

i. "an executing device link agent"

101. The '564 specification uses the term "agent" to refer to a component—which may, e.g., be "implemented… entirely in software" (EX-1001, 43:21-22)—that performs some function on behalf of an entity (e.g., a client or server). EX-1001, 15:53-16:7 (describing device agents that perform service policy implementation or management functions), 43:21-28 (agents talk to one another); *see also* EX-1029, 12 (computer science dictionary definition of agent). The specification does not set forth any ***required*** function. EX-1001, 15:64-16:7 ("It will be apparent to those of ordinary skill in the art that the division in functionality between one device agent and another is a design choice…."). In IPR2024-00341, the Board agreed that that the specification "uses the term 'agent' to include

components implemented 'entirely in software' to perform a function on behalf of a client or server." EX-1022, 27.

102. While the '564 specification never uses the term "***executing device link*** agent," it describes a "service control ***device link*** 1691," saying it may perform a "central agent communication hub function" (EX-1001, 42:9-15, 44:62-45:5) and "provides the device side of a system for transmission and reception" of messages, for example "service agent" messages "to/from network element functions" (EX-1001, 38:5-8).

103. MMS-Rakic's "MMS User Agent" is a device-side "application" (i.e., implemented in software) on TS-23.140's user device that receives and transmits messages to/from the MMS Relay/Server over MM1 and "***performs MMS-specific operations on a user's behalf and/or on another application's behalf***" (*see* my discussion above in Section VII.A, e.g., at paragraphs 44-49)—e.g., transportation of application-specific data to/from third-party VAS Applications via the Relay/Server. EX-1004, 14 (setting forth the standard's definitions, including for "abstract message," "application data," "MMS Relay/Server," "MMS User Agent," and "MMS VAS Application"), 19 (Section 5.1.1, describing MMS User Agent operations, including "transport of application data"), 23-24 (MMS architecture, showing interface MM1 between the MMS User Agent and the MMS Relay/Server), 30-31 (Section 7.1.3.1, Terminal Capability Negotiation, which

includes indicating whether the "MMS User Agent supports transporting application data"), 35-36 (Section 7.1.7, Support for Streaming in MMS, and describing types of data streaming that may be support), 41-42 (Section 7.1.13, Support for Value Added Services (VAS) in MMS), 54-56 (Section 7.1.18, Support for transporting Application Data).

104. MMS-Rakic's application-specific data is sent in what TS-23.140 calls "abstract messages." EX-1004, 14 ("abstract messages: information which is transferred between two MMS entities used to convey an MM and/or associated control information between these two entities."). MMS-Rakic's User Agent—which is an application on the MMS User Agent device that "performs MMS-specific operations on a user's behalf and/or on another application's behalf" (EX-1004, 14) and transports application data in the form of abstract messages (EX-1004, 14, 19, 54-56)—is thus a "device link agent," as claimed. This is consistent with the Board's finding in IPR2024-00341 that TS-23.140's MMS User Agent is "a service control ***device link agent*** on the end-user device[.]" EX-1022, 17-18.

105. Moreover, POSAs understood that MMS-Rakic's MMS User Agent application is an "***executing***" agent, because it is a software application that runs on TS-23.140's user device to perform various functions (*e.g.,* EX-1004, 19-20 (e.g., the functions listed in "5.1.1 MMS User Agent operations")) disclosed in TS-23.140. *See* EX-1046, 46 (defining ***application*** program: "A program ***executed***

with the processor in user mode."); EX-1045, 126 (defining ***execute***: "to run or carry out a computer program or process"), *id.* (defining ***execution***: "the process of carrying out a computer program or process").

ii. "respective executing processes for a plurality of software components"

106. As I discussed above in Section VII.D.1.c.i, MMS-Rakic's MMS User Agent application—i.e., the claimed "device link agent"—"performs MMS-specific operations on a user's behalf and/or ***on another application's behalf***." EX-1004, 14 ("MMS User Agent" definition). Among these operations is the "transport [of] data specific to application***s***—i.e., a ***plurality***—of applications "other than the MMS User Agent," that are also on MMS-Rakic's user device—for example, a "chess application" that "initially need[s] to register with the appropriate MMS User Agent" in order to send and receive such data. EX-1004, 14, 54-56 (*e.g.*, Section 7.1.18.1); EX-1028, 732-733 (Section 2.2, describing presence of multiple applications residing on a user device terminal, implemented to use MMS for transportation of application data). TS-23.140 discloses, for example, "received MMS information" (from, e.g., an MMS VAS Application) being "immediately routed" by the MMS User Agent "on to the destination application… without presentation to the user." EX-1004, 56 (Section 7.1.18.2.2).

107. MMS-Rakic's "other" destination applications (EX-1004, 14, 54) are separate from (and in communication with) the user device's MMS User Agent

application. EX-1028, 732-733) (contemplating, in the context of MMS, the presence of "multiple [destination] applications" on a mobile terminal); *see also* my discussion above in Section VII.C.3, paragraphs 71-77. The Board in IPR2024-00341 agreed. EX-1022, 30-31 ("[W]e find that an application residing on an MMS User Agent would also be understood as being differentiated from the MMS User Agent," and that "TS-23.140 discloses that its MMS User Agent and destination applications can be separate and in communication with each other…"). Confirming this is the fact that TS-23.140 discloses that the destination applications may be "downloadable… to a mobile phone" or "integrat[ed] into a mobile phone" through an "application registration process." EX-1004, 54 (Section 7.1.18, Support for transporting Application Data).

108. Based on TS-23.140's disclosures regarding destination applications—e.g., what they do (e.g., provide chess or news or weather services; EX-1004, 14, 55) and how they are added to a user device (e.g., by downloading to or integrating into a mobile phone; EX-1004, 54)—a POSA understood that TS-23.140's multiple destination applications (e.g., chess, news, and weather) are "a plurality of software components," as claimed. *See* EX-1046, 46 (defining ***application***: "A ***software*** program consisting of one or more processes and supporting functions."), *id.* (defining ***application*** program: "A program executed with the processor in user mode.").

109. The ’564 specification does not use the term “executing process” or discuss “respective executing processes for a plurality of software components.” However, a POSA understood that TS-23.140’s forwarding of application data to destination applications constitutes communications with “respective executing processes for a plurality of software components,” because a POSA understood that TS-23.140’s destination applications consisted of one or more processes in which specific functions of the application (e.g., receiving data) are executed. EX-1046, 46 (defining application: “a software program consisting of one or more processes and supporting functions”); EX-1047, 5:41-61 (“A software application can include multiple processes…”); EX-1048, [0003]-[0004] (describing “[d]ifferent processes within an application”).

110. For example, given a “chess” destination application, application data from an abstract message may be forwarded to, e.g., a specific process for moving the opponent’s chess pieces, or a specific “instance[]” of the “chess” application (e.g., “chess application #02”). EX-1004, 55-56. A POSA thus understood that MMS-Rakic’s MMS User Agent, which forwards application-specific data to various destination applications, communicates with “respective” “processes for a plurality of software components.” A POSA further understood that each respective process for MMS-Rakic’s destination applications is “executing” on TS-23.140’s device, as claimed, because they are software applications that run on TS-

23.140's device to perform the applications' respective functions. *See* EX-1046, 46 (defining ***application*** program: "A program ***executed*** with the processor in user mode."); EX-1045, 126 (defining ***execute***: "to run or carry out a computer program or process"), *id.* (defining ***execution***: "the process of carrying out a computer program or process").

iii. "an inter-process software communication bus providing secure communication between…"

111. Element [1B1] requires "an inter-process software communication bus providing secure communication between" the claimed "device link agent" (discussed above in Section VII.D.1.c.i) and "processes for a plurality of software components" (discussed above in Section VII.D.1.c.ii). The specification describes an "agent communication bus" that "can be implemented as an ***inter-process software communication bus***," which may be "***a variant of D-bus*** (e.g., a message bus system for inter-process software communication that, for example, helps applications/agents to talk to one another), or another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be secured, ***signed***, encrypted or otherwise protected." EX-1001, 43:21-31.

112. As discussed above in Section VII.C.3, TS-23.140 discloses its MMS User Agent receiving "data specific to an application other than the MMS User Agent" and "rout[ing]" it "to [a] destination application" on the user device over

some interface. EX-1004, 14, 54-56. In IPR2024-00341, PO was unable to "dispute that a destination application is in communication with an MMS User Agent," and the Board found that a POSA "would have… understood that [TS-23.140's] destination applications would have been communicatively coupled to the MMS User Agent by 'an agent communication bus,' as that term is used in the '733 patent, because they are, in the words of the '733 patent, 'talk[ing] to one another.'" EX-1022, 28-29; *see also id.*, 18-32; EX-1001, 43:24-31. A POSA therefore understood MMS-Rakic includes "an inter-process software communication bus providing… communication between" the MMS User Agent (the claimed "device link agent") and the one or more processes of the destination applications (the claimed "respective… processes"). *See* EX-1001, 42:14-43:44.

113. Separately, as discussed above in Section VII.C.3, it also would have been obvious to implement the interface between MMS-Rakic's MMS User Agent application and the respective processes of the user device's destination applications using a software ***bus*** for interprocess communications—e.g. a "D-bus." *See, e.g.*, EX-1031, 10:56-62 (disclosing a D-bus). As I noted above in Section VII.C.3 (see paragraph 77), the Board in IPR2024-00341 agreed this was obvious. The Board in IPR2024-00341 agreed that a software bus for interprocess communications would have been obvious over TS-23.140. EX-1022, 48-49. For

this alternative reason, MMS-Rakic includes an inter-process software communication bus.

114. MMS-Rakic's inter-process software communication bus also provides "***secure***" communication between an "executing device link agent and respective executing processes for a plurality of software components" because access to the bus is only allowed for software components identified by access authorization information received from a secure server, as I discuss further below in Section VII.D.1.d.

d. [1B2] wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and

115. The '564 specification only mentions "access authorization" once, when describing a "message… security framework technique[]… which ***only allows access to the agents that are on the secure authorization list*** and in which the list is provided by the secure server and ***signatures are provided by the secure server***[.]" EX-1001, 42:59-43:8. The specification only references the "secure server" in a single paragraph, which does not define any requirements for the "secure server." *See* EX-1001, 42:59-43:17 (describing the "secure server" solely by reference to exemplary functions it may perform, without imposing any

particular technical requirements or characteristics that would distinguish it from other servers performing those functions).

116. In MMS-Rakic, "providing secure communication comprises receiving access authorization information from a secure server," as claimed. MMS-Rakic's MMS User Agent receives application data from the MMS Relay/Server via MM1, in the form of "abstract messages" that each include an "application identifier of the destination application"—e.g., a "chess" application. EX-1004, 54-55 ("7.1.18 Support for transporting Application Data," "7.1.18.1 Application Identifiers," and "7.1.18.2.2 Receiving abstract messages"), 56 ("the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier"), 60 (Fig. 6, depicting an MMS User Agent's receipt of an MM1_retrieve.RES abstract message), 69 ("8.1.5.1 Normal Operation," describing the receipt of a MM1_retrieve.RES abstract message), 72-73 (Table 12, showing that the "Information elements in the MM1_retrieve.RES" include an "Applic-ID" that provides "Identification of the destination application"), 111 (Figure 8, depicting the flow of an abstract message from a VASP to an MMS User Agent as a MM7_submit.RES abstract message from the VASP to the MMS Relay/Server and a MM1_retrieve.RES abstract message from the MMS Relay/Server to the MMS User Agent). An MM1_Retrieve.RES message is a type of abstract message

which is sent from a MMS Relay Server to a MMS User Agent, after an MM identifying a destination application on a device upon which the MMS User Agent resides is received by the MMS Relay/Server (e.g., in the form of a MM7_submit.RES abstract message from the VASP), and "which contains MMs control information and the MM content." EX-1004, 69. The "application identifier" is the identifier that allows the User Agent to "immediately route[]" a received application-specific message to the corresponding one of the executing processes for a plurality of software components. EX-1004, 56.

117. As I discussed above in Section VII.C.4, MMS-Rakic's VAS Application incorporates the secure push message signing functionality of Rakic's "***secure*** push message server." In order to use that secure push message signing functionality to prepare a message comprising application-specific data to send to a destination application, MMS-Rakic's VAS Application generates a key by creating a hash of its administrator code and the destination application's identifier. EX-1007, [0041] ("using the codes may verify… that the client device includes a correct component."), [0042] ("The format of the secure push message… may be easily modified to accommodate different types of applications/devices that receive/send secure push messages."), [0048] (during initial configuration, the administrator device may obtain and store information that is specific to a client device, and client device may obtain and store administrator device's administrator

code), [0059] (client device components may include applications), [0066]-[0068] (Administrator device's secure push message server can generate a key based on codes obtained from the client device (e.g., a identifier) and the administrator device (e.g., an administrator code), and "[o]nce the key is generated, secure push message server 504 may generate an electronic signature based on the key and the message."), [0070]-[0071] (information associated with creating signatures may include, e.g., a client device identifier, an administrator code, and other information in "additional… different fields"), [0080] (describing the process for generating a key), [0085] (push message server may receive or generate the administrator code).

118. After the key is generated, MMS-Rakic's VAS Application uses the key to sign the message and generate a signature that is appended to the message. EX-1007, [0040] (the signature may be created by signing a message with a key), [0049] (same), [0067] ("secure push message server 504 may generate the secure push message by appending the electronic signature to the message"), [0079] (describing the process for generating a signature), [0105] (same), Fig. 8 (depicting a secure push message). As I discussed above in Section VII.A and further below in Sections VII.D.1.g and VII.D.1.h, MMS-Rakic's VAS Application then sends the signed message, via the Relay/Server, to the User Agent of the device on which the destination application resides. EX-1007, [0049]-[0050] (the signed message,

i.e., the secure push message, is sent to the target after signing), [0107] (same); EX-1004, 14, 17-18, 21 ("5.2 MMS Relay/Server"), 23-25 (discussing the MMS Reference Architecture, including MM1 and MM7 interfaces), 41 ("7.1.13 Support for Value Added Services (VAS) in MMS"). MMS-Rakic's VAS Application is a "secure server" as claimed because it incorporates the functionality of Rakic's "***secure*** push message ***server***" and because TS-23.140 discloses that communications with it (over MM7) are secured, e.g., using TLS (EX-1004, 41 ("For additional security, HTTP may be carried over a TLS [66] session to the MM7 interface.")).

119. A POSA understood that the MMS User Agent ("device link agent") of MMS-Rakic's device thus receives a message comprising an application identifier and a signature (collectively, "access authorization information") from the VAS Application ("secure server") which meets [1B2]'s "receiving access authorization information from a secure server" requirement because the MMS User Agent is an end-point of MMS-Rakic's inter-process software communication bus, over which application-specific data received from the network is "transported without alteration" (EX-1004, 14) to a destination application on the device.

120. A POSA further understood that, in MMS-Rakic, "access to the bus" is "allow[ed]… only for software components identified by the access authorization information," as claimed. As I discussed above in Section VII.C.4,

MMS-Rakic's User Agent incorporates the signature validation functionality of Rakic's secure push message client. After receiving the signed message, MMS-Rakic's User Agent generates a key by creating a hash of the administrator code (which was previously provisioned during destination application registration) and the destination application's identifier. EX-1007, [0110]-[0111] (describing the process of constructing the key using an identifier and the administrator code). After the key is generated, MMS-Rakic's User Agent signs the data block of the message with the key, and compares the resulting signature to the signature of the message. EX-1007, [0112] (describing the process of constructing the signature using the key). If the signatures match, the message is deemed valid and routed by MMS-Rakic's User Agent to the identified destination application. EX-1007, [0112]-[0119] (explaining that processing of the push message continues only if it is deemed valid by the secure push message client: "If the signed data block 804 is identical to the value of signature field 826, secure push message client 404 may determine that the secure push message is valid… if the secure push message is determined as a valid message, process 1402 may proceed to block 1412. Otherwise, process 1402 may terminate."), [0122] (describing a task performed when device receives push message), [0131] (similar); EX-1004, 54-56 ("7.1.18 Support for transporting Application Data," describing use and role of TS-23.140's "application identifier of the destination application" and "additional

application/implementation specific control information" in TS-23.140's "abstract message").

121. A POSA understood that the MMS User Agent ("device link agent") thus routes the message to the destination application ("software component") over MMS-Rakic's bus (see my discussion above in Section VII.D.1.c.iii) only if the signature (which, as discussed, is generated using the identifier that identifies the destination application) is valid. This meets [1B2]'s "allowing access to the bus only for software components identified by the access authorization information" requirement because the User Agent is an end-point of MMS-Rakic's inter-process software communication bus, over which application-specific data received from the network is "transported without alteration" (EX-1004, 14) to a destination application on the device.

e. [1C] the device link agent, configured to

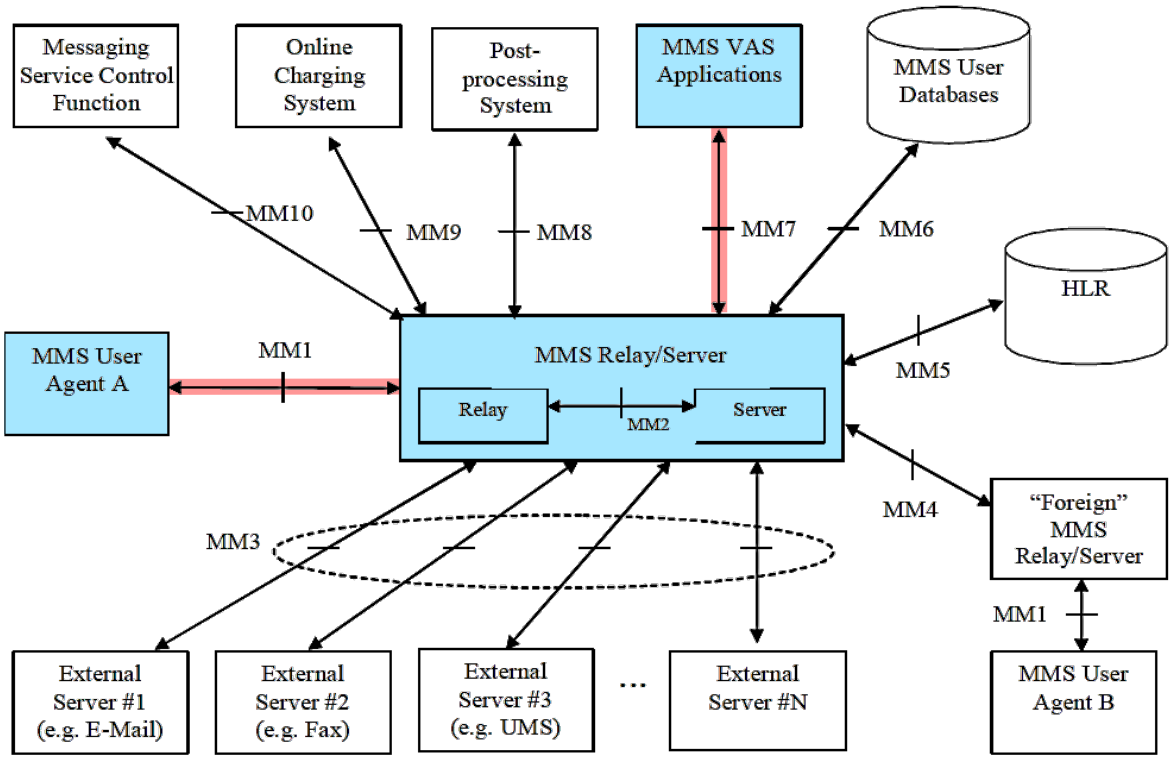
122. As I discussed above in Section VII.D.1.c.i, MMS-Rakic's User Agent is a "device link agent" and is implemented to incorporate the signature validation functionality of Rakic's secure push message client. As I explained below, MMS-Rakic's User Agent is configured to perform elements [1D1]-[1F].

f. [1D1] maintain a secure message link through the wireless network and an Internet network to a message link server,

123. The ’564 specification never describes a “message link server.” However, the specification refers to a “service control ***server link*** 1638,” which “provides the network side of a system for transmission and reception of service agent” messages and “provide[s]” a “***secure*** mechanism for transmitting and receiving” various types of “information between the device agents… and other network elements[.]” EX-1001, 69:16-56. Based on the claim’s plain language, a POSA understood that the claimed “***message link server***” includes a ***server*** with a ***link*** to the claimed device link agent, over which ***messages*** (e.g., between a device and another network element) are relayed. EX-1001, 16:13-16 (service controller 122 includes one or more server functions), 69:16-65 (describing functionality of the service control server link 1638 of FIG. 16).

124. As I discussed above in Section VII.A, TS-23.140 discloses that the MMS Relay/Server relays messages between the MMS User Agent and MMS VAS Applications using various communication interfaces between the MMS Relay/Server and other elements in the MMSE—*e.g.,* MM1 (EX-1004, 17-18, 21, 23-25) for communications between a MMS User Agent and MMS Relay/Server (*id.,* 23-24, FIG. 4), and MM7 for communications between the MMS Relay/Server and MMS VAS Applications (*id.*, 14, 18, 23-26, 41). *See* my

discussion in paragraphs 43-45 above. The path of messages between the VAS Applications and User Agent—through the Relay/Server—is annotated red below:



EX-1004, 23, FIG. 3 (annotated)

A POSA understood that, because MMS-Rakic's Relay/Server is a server that relays ***messages*** (e.g., between a device and another network element) to the MMS User Agent over ***link*** MM1, it is a "***message link server***," as claimed.

125. Element [1D1] also requires "a secure message link" between the "device link agent" and the "message link server." While the '564 specification does not use the term "secure message link," or require the connection between the claimed message link server and the claimed device link agent to be secured in any particular way, the specification describes a "service control link 1653" as the

connection between service control server link 1638 of service controller 122 and service control device link 1691 of service processor 115 that "provides for a ***secure (e.g., encrypted)*** communications link for providing secure, bidirectional communications…." EX-1001, 69:25-34; Fig. 16. The '564 specification leaves it to a POSA precisely how such a link is secured. For example, the '564 specification describes use of "***secure transport protocols running over Transmission Control Protocol (TCP)***," and notes that "approaches for implementing a secure control channel over the Internet includ[e]… running TCP Transport Layer Security (TLS)…." EX-1001, 16:66-17:22 ("…TCP provides a more reliable delivery channel for control traffic that is not as sensitive to delay or jitter."); *see also id.*, 89:29-36 (various known security encryption techniques can be used). The specification uses "TLS" and Secure Socket Layer (SSL) interchangeably. *E.g.*, EX-1001, 95:54 ("TLS/SSL"), 99:26 ("TLS/SSL"); 100:25 ("TLS/SSL"); 101:8-11 (providing "basic TCP setup, TLS/SSL" as example protocols used in "socket assignment and session management" layer in FIGS. 31-37).

126. As I discussed above in Section VII.D.1.c.i, in MMS-Rakic, the MMS User Agent (the claimed "device link agent") communicates with the MMS Relay/Server (the claimed "message link server") over interface MM1. And as I discussed above in Section VII.C.2, MMS-Rakic's MM1 interface is secured using

SSL/TLS. *See also* EX-1004, 24-25 (describing the MM1 interface between the MMS User Agent and the MMS Relay/Server); EX-1012, 21 ("[t]he ***TLS*** [WP-TLS] transport layer security protocol ***provides for secure data transmission between the MMS Client and the MMS Proxy-Relay*** in architectural configurations that employ HTTP based protocol stacks for MMS_M implementation"). A POSA understood MMS-Rakic's MM1 is thus a "secure message link" between the User Agent and Relay/Server, as claimed.

127. Element [1D1] also requires the claimed "device link agent" (MMS User Agent) to "***maintain***" the "secure message link." The '564 specification leaves it to a POSA precisely how a "device link agent" "***maintain[s]*** a secure message link," saying only that the "the service control device link 1691 ***provides the device side of a system for transmission and reception of service agent to/from network element functions***." EX-1001, 38:5-8. As I discussed above in Section VII.D.1.c.i, MMS-Rakic's MMS User Agent ***provides*** the device side of MMS-Rakic's system for transmitting and receiving messages on behalf of destination applications from VAS Applications, which includes MM1 between the MMS User Agent and MMS Relay/Server. MMS-Rakic's MMS User Agent thus "maintain[s] a secure message link" to the MMS Relay/Server in the same way that the specification discloses.

128. Element [1D1] further requires that the "secure message link" be maintained "***through the wireless network and an Internet network***." As I discussed above in Section VII.D.1.b, MMS-Rakic's MMS User Agent communicates with the MMS Relay/Server over the MM1 interface through a "wireless network" (e.g., a 2G or 3G mobile network). TS-23.140 discloses "that multimedia messaging may encompass many different network types[,]" and "[t]he basis of ***connectivity*** between these different networks shall be provided by the ***Internet protocol*** and its associated set of messaging protocols," which "enables messaging in 2G and 3G ***wireless networks to be compatible with messaging systems found on the Internet***." EX-1004, 17, 18 ("MMS connectivity across different networks (MMSEs) is provided based on ***Internet*** protocols."). A POSA thus understood that each of TS-23.140's wireless ***networks*** (e.g., 3G Mobile Network A), which must be communicated over via the "***Internet protocol*** and its associated set of messaging protocols," is also "an Internet network." Thus, a POSA understood that MMS-Rakic's "secure" MM1 interface is also "maintain[ed]… through" "an Internet network to" the MMS Relay/Server (the claimed "message link server").

129. TS-23.140 further teaches a "secure message link" that is "maintain[ed]" "through" "an Internet network" that is ***separate*** from "the wireless network." TS-23.140 says the "[MMS] architecture… shall ***combine <u>different</u>***

networks and network types and shall integrate messaging systems already existent within these networks[,]" and that "connectivity between these different networks shall be provided by the ***Internet protocol*** and its… messaging protocols." EX-1004, 16-17. TS-23.140 does not limit the ways in which communications are facilitated over such networks or what "network types" the MMS "architecture… shall ***combine***." *E.g.*, EX-1004, 16-17 ("The basis of connectivity between these different networks shall be provided ***by the Internet protocol*** and its associated set of messaging protocols. This approach enables messaging in 2G and 3G wireless networks ***to be compatible with messaging systems found on the Internet***."), 23-24 ("MMS shall make use of [a] protocol framework outlined in figure 4. In this framework the MMS User Agent communicates with the MMS Relay/Server, which may communicate with External Servers. This MMS Relay/Server may provide convergence functionality between External Servers and MMS User Agents and thus enables the integration of different server types across different networks."). A POSA understood, based on these disclosures, that TS-23.140 discloses scenarios in which a user device's MM1 interface encompasses multiple different networks that have been combined to communicate with MMS-Rakic's Relay/Server—e.g., the wireless network of element [1A] ***and*** a separate network that also uses Internet protocol, as TS-23.140 teaches (EX-1004, 16-17). For such an implementation of MM1, encompassing a "combine[d] different networks" as

TS-23.140 teaches (EX-1004, 16-17), a POSA understood that the "secure message link" (MM1) is "maintain[ed]" by the User Agent "through the wireless network" of [1A] and a separate "Internet network."

130. Moreover, implementing MMS-Rakic's User Agent device to be able to connect to the Relay/Server through both a wireless network and a separate Internet network would have been obvious to a POSA. It was well-documented to implement mobile user devices to connect to a ***wireless*** local area network that is connected to the Internet in order to allow the user device to communicate with a remote server. *E.g.*, Cole (EX-1006), [0031]-[0035], FIG. 1 (showing and describing mobile device 110 connecting to remote server 195 through public network 170, which may be the "Internet"). A POSA understood that such an implementation of MMS-Rakic—e.g., where a User Agent device is implemented to connect to a WLAN which connects to the Internet in order to allow the user device to communicate with the Relay/Server—would have desirably provided an additional access path to the Relay/Server using existing IP-based MMS protocols, thereby improving the device's accessibility to MMS in environments where 2G/3G cellular coverage was weak, unavailable, or costly—resulting in increased user flexibility and connectivity for MMS services. Moreover, because a POSA understood that the Internet is itself a network of interconnected networks—and TS-23.140 provides that connectivity between "different networks and network

types" "shall be provided by the Internet protocol and its… messaging protocols" (EX-1004, 16–17)—a POSA would have expected that maintaining MMS communications "through" an Internet network would involve traversing multiple distinct networks between the MMS User Agent and the MMS Relay/Server, and based on this would have found it desirable and obvious to maintain MMS-Rakic's secure message link MM1 across both the wireless network and an Internet network as part of an end-to-end IP-based MMS communication path. A POSA would have reasonably expected success with such an implementation, because maintaining links between network entities over multiple distinct networks that comprise the Internet was expected and common at the time of the Critical Date, as TS-23.140's own disclosures confirm (EX-1004, 16-17), and well within a POSA's ability to implement.

g. [1D2] the message link server operating a message service that receives messages over a network from a plurality of network functions,

131. The '564 specification never uses the term "message service," or describes what it means for a "message link server" to "operat[e]" one. Based on the claim's plain language, a POSA understood "operating a message service" to include a service that facilitates the receipt and transmission of messages over a network by [1C]'s device link agent. *See* EX-1001, 69:34-37 (referring to a "service control server link 1638 [that] provides the network side of a system for

transmission and reception of service agent [messages] to/from network element functions[.]").

132. A POSA understood that MMS-Rakic's Relay/Server (the claimed "message link server") operates a message service. As I discussed above in Sections VII.A, VII.D.1.d, and VII.D.1.f, MMS-Rakic's Relay/Server relays signed messages between MMS-Rakic's MMS User Agent (the claimed "device link agent") and, e.g., MMS VAS Applications. EX-1004, 14, 17-18, 21, 23-26, 41, FIG. 3. As I discuss below, MMS-Rakic's VAS Applications comprise "network functions" which send messages to MMS-Rakic's User Agent.

133. The '564 specification uses "network function" to encompass any network element that provides some function (e.g. to another network element or to a user) over the network. EX-1001, 80:12-20 ("a ***network function*** (e.g., the service controller 122, and/or more specifically the policy management server 1652 ***function***, or other similar ***function***)… program[s]… the various ***network*** apparatus ***functions*** (e.g., possibly including but not limited to the service controller 122 or similar ***functions***…)"); *see also id.*, 38:5-8 ("the service control device link 1691 provides the device side of a system for transmission and reception of service agent [messages] to/from ***network element functions***."), 69:34-37 ("In some embodiments, the service control server link 1638 provides the

network side of a system for transmission and reception of service agent to/from ***network element functions***.”), 79:44-46.

134. MMS-Rakic’s VAS Applications are “network elements” that provide a function over the MMSE network. FIG. 2, showing TS-23.140’s MMSE which includes “***a collection of MMS-specific network elements***” that communicate with one another, is below:

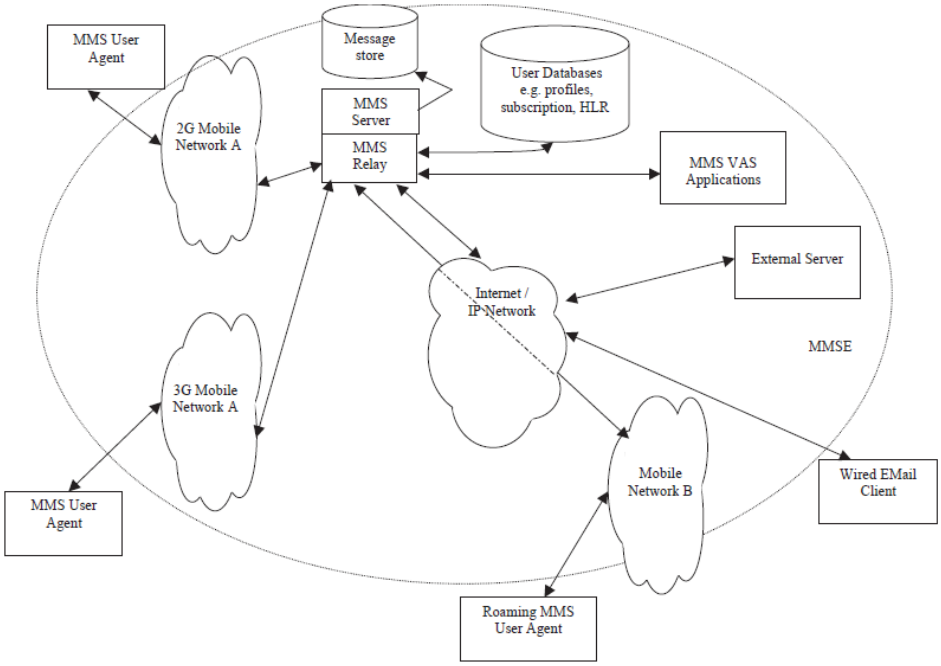


Figure 2: MMS Architectural Elements

EX-1004, 17, FIG. 2

MMS VAS Applications provide various functions “to MMS users” over the MMSE network—e.g., “Value Added Services (e.g. news service or weather forecasts).” EX-1004, 14 (defining “MMS VAS Applications”), 23 (Section 5.6, “MMS VAS Applications”). As I discussed above in Section VII.D.1.c.i, MMS VAS Applications transport application-specific data sent in “abstract messages” to

destination applications on user devices via the MMS Relay/Server and each user device's respective MMS User Agent. EX-1004, 14 ("abstract messages: information which is transferred between two MMS entities used to convey an MM and/or associated control information between these two entities."), 19, 23-24 (Section 6.1, describing the MMS Architecture), 30-31, 35-36, 41 ("The MMS Relay/Server may support services, in addition to user-to-user messaging, that are… provided… by third-party Value Added Service Providers (VASP)[,]" such as "[m]essages that originate from the VASP to a single… recipient[.]"), 54-56 (discussing using "abstract messages" to "transport application data"). "There could be ***several*** MMS VAS Applications included in or connected to an MMSE." EX-1004, 18.

135. Because MMS-Rakic's MMS VAS Applications are network elements that provide value added services over the MMSE to destination applications, a POSA understood that the MMS VAS Applications constitute "a plurality of network functions." As I discussed above in Sections VII.D.1.f and VII.D.1.d, MMS-Rakic's MMS Relay/Server receives messages from the MMS VAS Applications over MM7 within the MMSE network. A POSA thus understood that MMS-Rakic's MMS Relay/Server (the claimed "message link server") "operat[es] a message service" that "receives messages over a network,"

as claimed, from the MMS VAS Applications (the claimed "plurality of network functions").

h. [1E]

136. MMS-Rakic meets each limitation in Element [1E], as I discuss below.

i. receive secure messages from the message link server over the secure message link

137. As I discussed above in Section VII.D.1.f, MMS-Rakic's MMS User Agent (the claimed "device link agent") maintains interface MM1 (the claimed "secure message link") to the MMS Relay/Server (the claimed "message link server"), over which MMS-Rakic's User Agent receives messages, as I discussed above in Section VII.D.1.c.i. Such messages received over MM1 are "secure[d]" at least using SSL/TLS, because MMS-Rakic's MM1 between the MMS User Agent and the MMS Relay/Server is secured using SSL/TLS (as I discussed above in Section VII.C.2). They are also signed, in view of Rakic's teachings (as I discussed above in Section VII.C.4). A POSA understood that MMS-Rakic's MMS User Agent thus "receive[s] secure messages from the message link server over the secure message link."

138. Rakic also discloses its signed messages—which in MMS-Rakic are received from the Relay/Server over interface MM1 (as I discussed above in Sections VII.D.1.d and VII.D.1.g)—being encrypted, as I discussed above in

Section VII.B and discuss further below in Section VII.D.7. EX-1007, [0075] (disclosing messages secured using "a combination of generating a signature ***and encrypting the data***" in the payload), [0078] ("Data field 822 may include content (e.g., payload)"). A POSA understood that such messages received "from the message link server over the secure message link" in MMS-Rakic—e.g., those "encrypted" as Rakic contemplates, in addition to being secured by virtue of applying SSL/TLS to MM1 and signed in view of Rakic—were secure for this additional reason.

ii. the received messages identified for delivery to multiple ones of the software components, and

139. As discussed above in Section VII.D.1.c.i, in MMS-Rakic, MMS is "used to transport data specific to application**s**" on the user device that are not the MMS User Agent. EX-1004, 54-56 (Section 7.1.18, Support for transporting Application Data, describing MMS User Agent's sending and receiving of abstract messages); *see also* EX-1028, 732-733 (describing the use of MMS to transport application data between peer applications). See my discussion above in Section VII.A. Also, as I discussed above in Section VII.D.1.c.ii, MMS-Rakic's destination applications are "a plurality of software components," as claimed. A POSA understood that each such destination application is thus one of "multiple… software components" on the device.

140. As I discussed above in Section VII.D.1.d, the messages received by MMS-Rakic's User Agent are in the form of "abstract messages" that comprise access authorization information including a signature and an "application identifier of the destination application" that allows the User Agent to "immediately route[]" each message to the one "destination application" (of the device's multiple destination applications) "that is referred to from the destination application identifier." EX-1004, 56. Because MMS is used in MMS-Rakic to transport data specific to applications—and because this routing takes place using an application identifier "present in [each] abstract message" (EX-1004, 55) sent by the MMS Relay/Server to the MMS User Agent—a POSA understood that "the received messages [are] identified for delivery to multiple ones of the software components," as claimed.

iii. including message content received by the message link server from multiple ones of the network functions, and

141. As I discussed above in Sections VII.D.1.c.i-VII.D.1.c.ii, MMS-Rakic's secure messages (including the "abstract messages" I discussed above in Sections VII.D.1.c.i, VII.D.1.d, and VII.D.1.g) are "used to transport data specific to applications" other than the MMS User Agent. EX-1004, 54-56 (describing MMS User Agent's sending and receiving of abstract messages); *see also* EX-

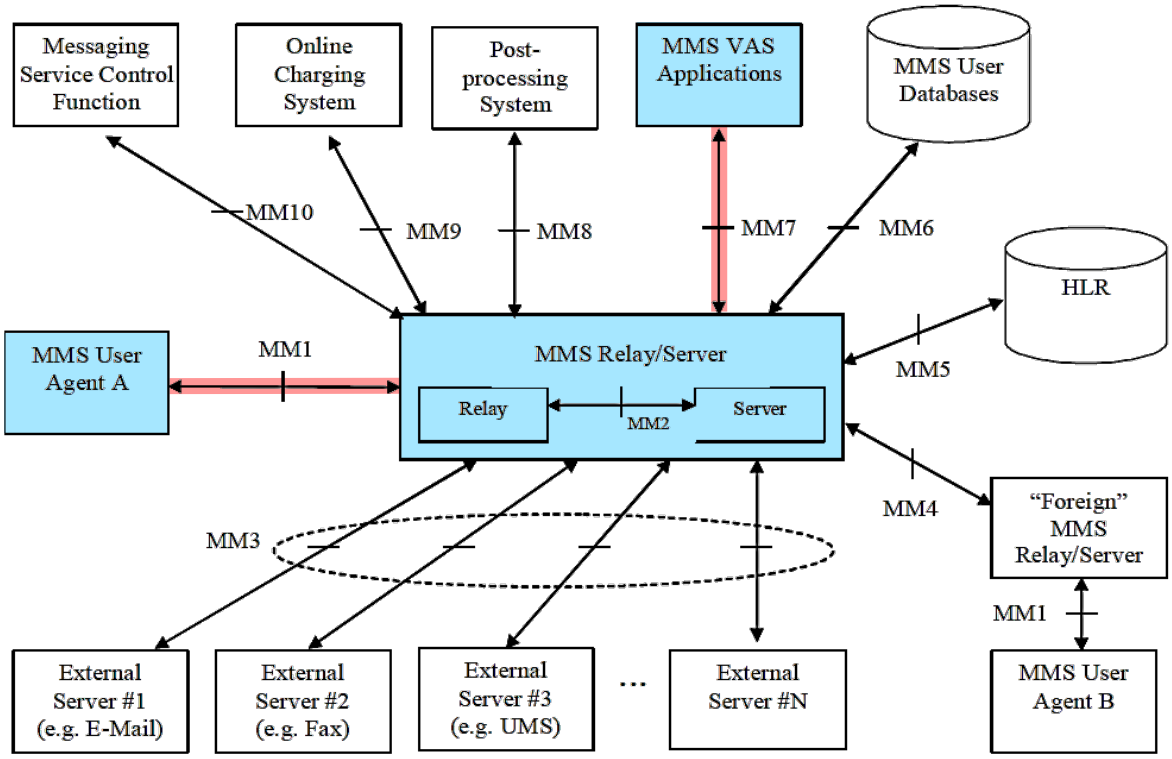
1028, 732-733 (describing the use of MMS to transport application data between peer applications). See also my discussion above in Section VII.A.

142. TS-23.140 states that such "Application Data may be of any ***content*** type[.]" EX-1004, 14, 54-56 (disclosing "transporting" such "Application Data" in "abstract messages"). TS-23.140 also discloses that the "abstract messages" sent by VAS Applications for delivery by the MMS Relay/Server to the MMS User Agent include "content." EX-1004, 69-70 (MM1_retrieve.RES messages may contain content for delivery to the MMS User Agent), 112-113 ("The VASP may add content in the MM7_submit.REQ" message for delivery to the MMS User Agent via the MMS Relay/Server). A POSA thus understood that TS-23.140's "application data" (i.e., application-specific data)—which is transported in MMS-Rakic's messages (e.g., abstract messages) to specific applications "without alteration" (EX-1004, 14 ("Application Data: Information / data specific to an application other than the MMS User Agent / VASP which ***is intended to be transported without alteration*** by using MMS."), 54-56)—constitute "***message content***" as claimed.

143. A POSA further understood that abstract messages (with "message content") received by MMS-Rakic's MMS User Agent (the claimed "device link agent") are "received by the" MMS Relay/Server (the claimed "message link

server") "from multiple ones of the" VAS Applications (the claimed "network functions"), as claimed.

144. MMS-Rakic's messages containing application data (including the "abstract messages" I discussed above in Sections VII.D.1.c.i, VII.D.1.d, and VII.D.1.g) include data from various VAS Applications. EX-1004, 14 (defining "application data"), 18 ("VAS Applications offer Value Added Services to MMS users"), 23 (Section 5.6, describing MMS VAS Applications), 41 ("The MMS Relay/Server may support services… provided… by third-party [VASPs]. … Messages originated from the VASP may be targeted to the recipient…"), 54-56 (Section 7.1.18, "Support for transporting Application Data"). These messages contain "application data" used to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users." EX-1004, 14, 41; Section VII.A. I have annotated the path of application data between the VAS Applications and User Agent in red below:



EX-1004, 23, FIG. 3 (annotated)

Above, application data is transmitted by ***multiple*** "VAS application***s***" to the MMS Relay/Server via interface MM7, then relayed "without alteration" (EX-1004, 14) to the MMS User Agent via interface MM1, and then routed internally to various specific destination applications. EX-1004, 14, 18, 23-25, 41, 54-56 ("If the destination application resides on a receiving MMS User Agent, the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier… without presentation to the user."), FIG. 8 (below).

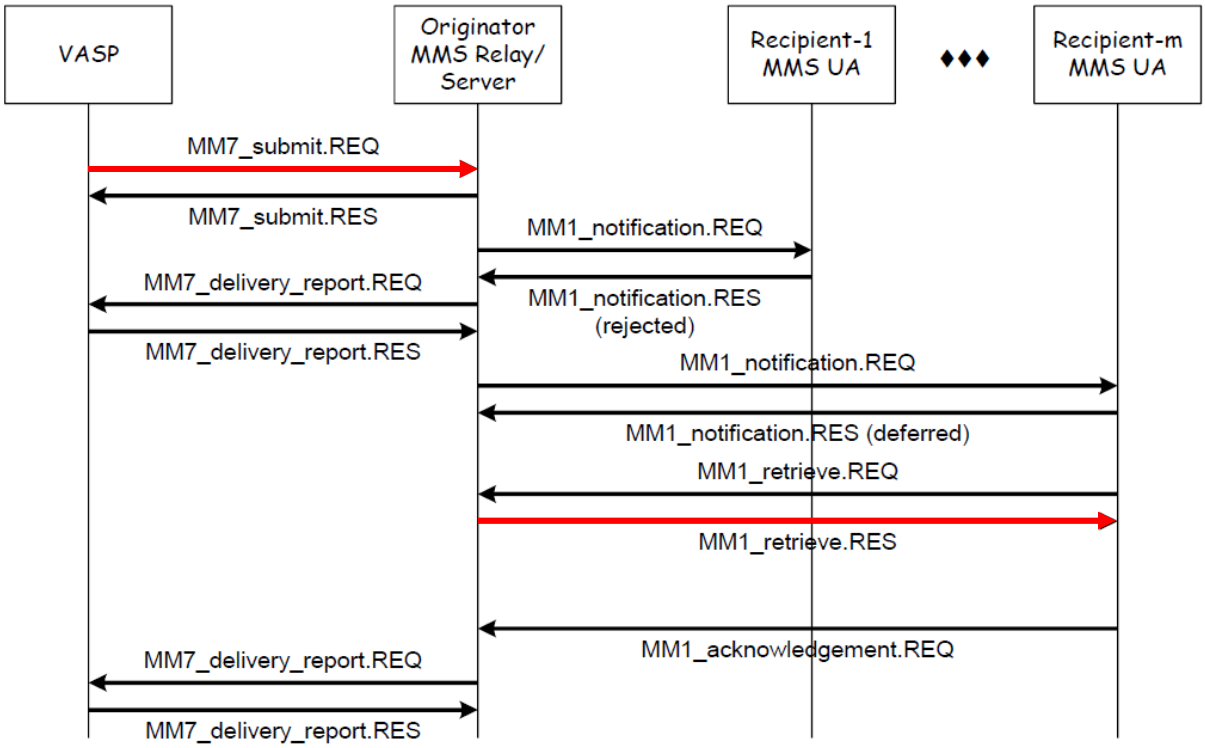


Figure 8. Sample data flow of MM7 message distribution

EX-1004, 111, FIG. 8 (annotated)

See also EX-1004, 111-116 (describing VASP-added "Content" and "Applic-ID… indicat[ing] that… abstract message shall be provided to an application residing on an MMS User Agent" in MM7_submit.REQ), 69-73 (describing "Content" conveyed from originator and "Applic-ID" in MM1_retrieve.RES). The Board in IPR2024-00341 agreed with Petitioner that "application-specific data from VAS applications" is "provided" to user agents "by VAS providers communicating through the MMS Relay/Server." EX-1022, 38 (citing EX-1004, 23-24, 25-26, 41, 112, FIG. 3).

i. [1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component.

145. MMS-Rakic's MMS User Agent—for "messages identified for delivery to a given one of those software components"—"route[s the] messages" "via the inter-process software communication bus to a software process corresponding to the given software component." In IPR2024-00341, relying on the teachings of TS 23.140, the Board found that the prior art disclosed substantially the same limitation in the '733 Patent. EX-1022, 39-40, §II.D.3(m).

146. In particular, MMS-Rakic's MMS User Agent "transport[s]" application-specific messages (including the "abstract messages" I discussed above in Section VII.D.1.h) by "***rout[ing]***"—"without alteration"—"received MMS information on to the destination application that ***is referred to by the destination application identifier***" included in the received messages. EX-1004, 55-56; *see also id.* at 14 (defining "abstract message" and "application data"). As I discussed above in Sections VII.C.3 and VII.D.1.c.iii, these messages are routed over "an inter-process software communication bus providing secure communication between" MMS-Rakic's User Agent and the one or more processes (as I discussed above in Section VII.D.1.c.ii) of the destination applications.

147. A POSA understood that the "messages [are] identified for delivery to a given one of those" destination applications (the claimed "software component"), as claimed, because MMS-Rakic's MMS User Agent routes each message to the application "***referred to***" (EX-1004, 54) by the application identifier. A POSA thus understood that, for "messages identified for delivery to a given one of those software components" (including each abstract message I discussed above in Section VII.D.1.h), the MMS User Agent (the claimed "***device link agent***," discussed above in Section VII.D.1.c.i), "***route[s]***" the "messages" to a software process of the identified destination application ("***to a software process corresponding to the given software component***") "via the inter-process software communication bus," as claimed.

148. A POSA also understood MMS-Rakic's MMS User Agent only "route[s] messages" "for software components identified by the access authorization information." As I discussed above in Section VII.D.1.d, the MMS User Agent only routes received messages to the identified destination application over MMS-Rakic's bus if the signature (which is generated using the identifier that identifies the destination application) is deemed valid. EX-1007, [0112] ("If the signed data block 804 is identical to the value of signature field 826, secure push message client 404 may determine that the secure push message is valid."), [0113]-[0119], [0122], [0131] (describing the device acting on the received secure

message after secure push message client determines that the secure push message is valid); EX-1004, 54-56 (discussing transport of application data to an intended destination application using "application identifier" for destination application).

2. Claim 2: The mobile end-user device of claim 1, wherein the access authorization information provided by the secure server for a given one of the software components comprises a signature.

149. Claim 2 requires that the "access authorization information provided by the secure server for a given one of the software components comprises a signature." As I discussed above in Sections VII.D.1.d and VII.C.4, MMS-Rakic's "access authorization information"—which is "provided" in MMS-Rakic's abstract messages "by the secure server" that corresponds to "a given one of the software components"—includes both an application identifier and a signature (see my discussion above in paragraphs 116-119). Because the "access authorization information" includes MMS-Rakic's signature, it "***comprises***" MMS-Rakic's "***signature***" and meets claim 2.

3. Claim 3: The mobile end-user device of claim 1, wherein the software components include a first device component that receives message content in a first format, and a second device component that receives message content in a second format different than the first format.

150. Claim 3 requires claim 1's "software components" to "include" a "first" and "second" "device component" that respectively "receive[] message content" in different "format[s.]" TS-23.140 discloses a "[m]inimum set of

supported formats," e.g., "Plain Text," "Audio," "Still Image," and "Video." EX-1004, 20; EX-1020 (3GPP TS-26.140 (Multimedia Messaging Service; Media formats and codecs)). A POSA understood that MMS-Rakic's different applications (e.g., "chess," "weather") comprise "components" on the "device" that would receive application data in different formats specific to the respective applications, and thus would meet claim 3. For example, a POSA understood that TS-23.140's chess application (a "first" application) is a device component that would receive application data in a "first" format that is used by the chess application (e.g., a format suitable for transmitting data about an opponent's chess move), while TS-23.140's weather application (a "second" application) is a device component that would receive application data in a "second" format that is used by the weather application (e.g., a format suitable for transmitting data about an upcoming hurricane). EX-1004, 14, 55. It would have been desirable to a POSA to implement MMS-Rakic to be able to receive data in different formats specific to such applications, as this would have helped the MMS-Rakic device facilitate provision of a variety of services from different VASPs to the user. EX-1004, 14, 54-56. A POSA would have reasonably expected doing so, in view of TS-23.140's disclosure of implementing MMS such that it can support the handling of different data formats (EX-1004, 20) and the transport of data specific to different types of applications (EX-1004, 14, 55).

4. Claim 4: The mobile end-user device of claim 3, further comprising a user interface, wherein the first device component is a user service interface agent, and the first format comprises a notification message, the user service interface agent configured to display the notification message on the user interface.

151. Claim 4 depends from claim 3. Claim 4 requires "a user interface," specifies that claim 3's "first format comprises a notification message," and specifies that the "first device component" is "a user service interface agent configured to display the notification message on the user interface."

152. A POSA understood that TS-23.140 discloses functionality that confirms the presence of a user interface in TS-23.140's user device. For example, TS-23.140 describes "MM ***presentation***" (where the MM is "***displayed*** to the end user") and "***presentation*** of notifications to the user," e.g., in an "manual" "retrieval mode[]," where "the end user" is "made aware of the MM notification and… allowed to make a decision whether to download the MM[.]" EX-1004, 19-20. Moreover, every depiction of a device comprising an MMS User Agent in TS-23.140 comprises a user interface, e.g. a display. EX-1004, 16 (Figure 1, showing end-user devices including displays and keyboards/keypads), 155-160 (Figures A.1-A.8, showing touchscreens/styluses), 173 (Figure E.1).

153. The use of user interfaces on devices to facilitate content presentation to users was well-documented. For example, as I discussed above in Section VII.B, Rakic discloses a "client device" with a display "provid[ing] visual information to

the user" and control buttons "permit[ting] the user to interact with [the] client device[.]" EX-1007, [0052]. A POSA thus understood TS-23.140's user device includes a "user interface," as claimed. Alternatively, such an implementation would have been an obvious way to implement what TS-23.140 describes, and is nothing more than using familiar, known components (a user interface on, e.g., a display) to achieve a predictable result of facilitating content-presentation to a user.

154. A POSA further understood that TS-23.140 also discloses a destination application receiving "notification" messages. For example, a MM1_notification.REQ abstract message with a "destination application identifier" is sent to the MMS User Agent to notify the destination application of an incoming MM (which may later be sent in a MM1_retrieve.RES abstract message, e.g., as discussed at EX-1004, 69-71). EX-1004, 56 ("an abstract message containing a destination application identifier… can… be the MM1_notification.REQ" and "When an MM is addressed to an application, the associated MMS notification, intended for this application, should contain the application identifier."), 60 (Figure 6, showing the transmission of a MM1_notification.REQ abstract message from a MMS Relay/Server to a MMS User Agent), 61 (same), 66-68 (Section 8.1.4, "Multimedia Message Notification," stating a MM1_notification.REQ may contain an "Applic-ID [that] contains the identification of the destination application. Upon reception, the recipient MMS

User Agent shall provide this MM1_notification.REQ to the specified destination application."). Upon receiving such a MM1_notification.REQ message with a "destination application identifier," "the MMS User Agent… ***immediately route[s]***" it "to the [identified] destination application… without presentation to the user." EX-1004, 56.

155. As I noted above, TS-23.140 discloses "retrieval of MMs in a manual… fashion," where the "end user is made aware of the MM notification and is allowed to make a decision whether to download the MM or not." EX-1004, 19-20. TS-23.140 thus contemplates scenarios in which the MMS User Agent routes a notification message intended to be presented to a user to a destination application without the MMS User Agent first presenting it to the user. EX-1004, 56 ("an abstract message containing a destination application identifier… can… be the MM1_notification.REQ" and "When an MM is addressed to an application, the associated MMS notification, intended for this application, should contain the application identifier" and "If the destination application resides on a receiving MMS User Agent, the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier… ***without presentation to the user***."), 66-68 (Section 8.1.4, "Multimedia Message Notification," stating a MM1_notification.REQ may contain an "Applic-ID [that] contains the

identification of the destination application. Upon reception, the recipient MMS User Agent shall provide this MM1_notification.REQ to the specified destination application.”). A POSA understood that in such a scenario, the destination application that receives the notification message is responsible for presenting the notification message to the user using the user interface of TS-23.140’s user device.

156. A POSA understood that such a destination application in MMS-Rakic (which receives a MM1_notification.REQ message and displays the notification to a user, as described above) constitutes a “***user service interface agent*** configured to display the notification message on the user interface,” as claimed. The specification uses “user service interface agent” to include an agent that “provide[s a] service [and/or user] interface to users.” EX-1001, Fig 22B (“***User Interface Agent*** 1697” “Provide[s] ***service interface*** to users.”); 66:35-36 (using “service interface” and “user interface” interchangeably); 96:39-42 (“communicates… user input to the user service interface agent”), 97:65-67 (“the user can be notified… via the user service interface agent”). And each destination application in MMS-Rakic described above (1) is an ***agent*** because, as I discussed above in Sections VII.D.1.c.i and VII.D.1.c.ii, it is a component implemented in software that perform some function on behalf of an entity (e.g., client, server), (2) receives “Value Added ***Services***” from VAS Applications (as I discussed above in

Section VII.D.1.g), and (3) as discussed above, presents the notification using MMS-Rakic's ***user interface***, meeting claim 4.

5. Claim 5: The mobile end-user device of claim 4, the user service interface agent further configured to obtain a user input as a response to the display of the notification message, and deliver the user input to an agent on the device.

157. Claim 5 requires that claim 4's "user service interface agent" be "configured to obtain a user input as a response to [claim 4's] display of the notification message, and deliver the user input to an agent on the device."

158. In the "manual" MM retrieval mode of MMS-Rakic I discussed above in Section VII.D.4, "the end user is made aware of" a "MM notification" and "***allowed to make a decision whether to download the MM or not***." EX-1004, 19-20. TS-23.140 discloses the MMS User Agent retrieving the MM from the MMS Relay/Server by (1) responding to the MM1_notification.REQ message with a MM1_notification.RES message, and (2) requesting download of the MM by sending a MM1_retrieve.REQ message. EX-1004, 60 (Figure 6, illustrating the exchange of MM1_notification.REQ, MM1_notification.RES message, and MM1_retrieve.REQ abstract messages), 66 (describing MM1_notification.REQ and MM1_notification.RES messages), 69 (describing MM1_retrieve.REQ messages). TS-23.140 also explains that "an application" on TS-23.140's user device "may trigger an MMS User Agent… to submit" such "abstract messages,"

where the MMS User Agent "insert[s]" information "receive[d]… from the application" into an "abstract message" and sends it. EX-1004, 55.

159. In Section VII.D.4 above, I discussed the scenario where the destination application is forwarded the MM1_notification.REQ message without presentation by the MMS User Agent, and that a POSA thus understood that the destination application is responsible for presenting the MM notification to the user. In this scenario, a POSA would have been motivated to implement (and would have reasonably expected success implementing) the destination application to (1) receive the user's decision whether to download the MM, and (2) trigger the MMS User Agent to submit the MM1_notification.RES and MM1_retrieve.REQ messages to the MMS Relay/Server, because this was consistent with TS-23.140's teachings (discussed in Section VII.D.4 above) and an efficient, straightforward way of receiving the user's decision regarding whether to download an MM. As I discussed above in Section VII.D.1.c.i, MMS-Rakic's User Agent is an ***agent*** on the device. Thus, a POSA understood that the destination application that receives the MM1_notification.REQ message obtains the user's decision (the claimed "user input") in response to presenting the MM notification, and delivers "the user input" to the MMS User Agent ("an agent on the device"), meeting claim 5.

6. Claim 6: The mobile end-user device of claim 3, wherein the first device component is a policy control agent, and the first format contains service settings and/or configuration information.

160. Claim 6 depends from claim 3 and recites that "the first device component is a policy control agent," and that "the first format contains service settings and/or configuration information." The '564 specification describes a "policy control agent" to include an agent that "[t]akes policy instructions from the network" and "adapts device service policy settings (e.g., instantaneous device service policy settings)." EX-1001, Fig. 22A, 48:31-38.

161. A POSA understood that MMS-Rakic's device comprises a "policy control agent" that receives "service settings and/or configuration information" over a network from components of the MMSE. In particular, TS-23.140 discloses MMS User Databases "that… contain user related information such as subscription and configuration" data, user profiles, access controls, server storage space, delivery rules, and user device capabilities. EX-1004, 18, 22 (Section 5.5, describing the functionality "MMS User Databases" "shall provide"). MMS User Databases are "network elements" that provide a function over the MMSE network and thus constitute "network functions." *See* my discussion above in ¶133. As shown below, MMS User Agents interface with MMS User Databases (through the MMS Relay/Server) using MM1 and MM6 (which I have annotated in Figure 3 of TS-23.140 in red below).

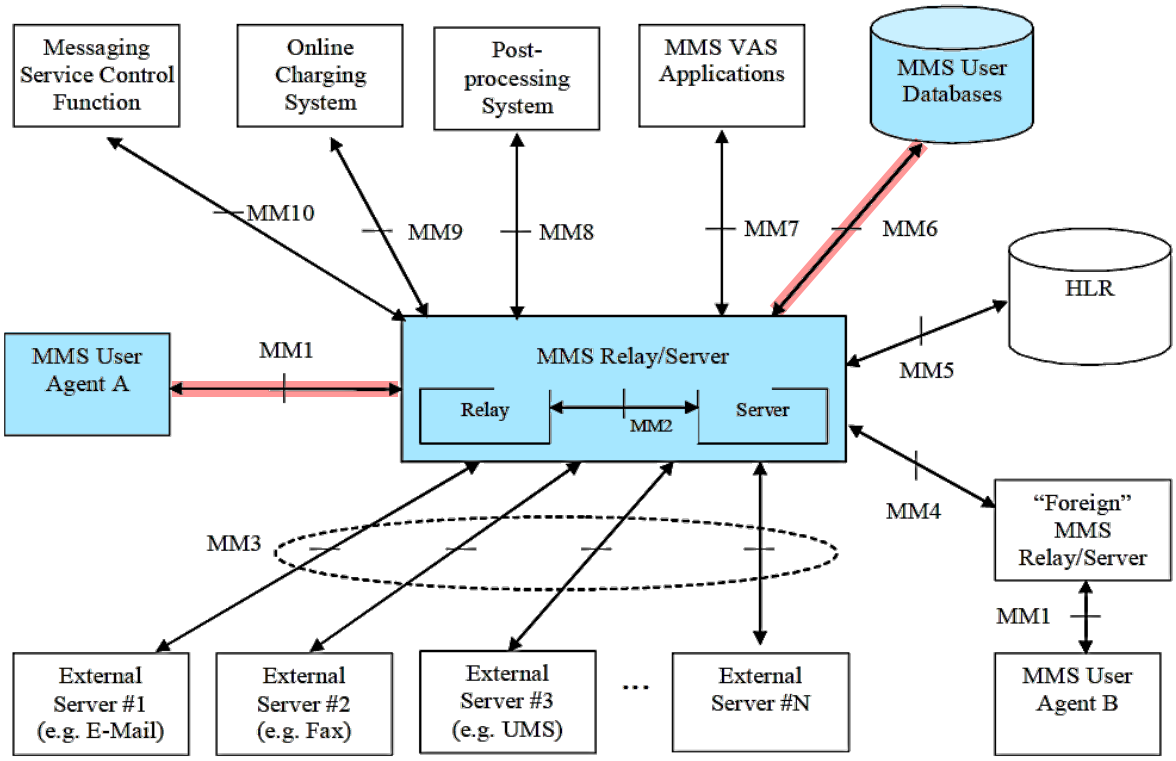


Figure 3: MMS Reference Architecture

EX-1004, 23, FIG. 3 (annotated)

EX-1004, 23-24 ("MM6: The reference point between the MMS Relay/Server and the MMS User Databases").

162. Moreover, contemporaneous references discussing MMS confirm that TS-23.140's device routinely processed device settings and policies that are updated and communicated (through push messages) by the MMS User Databases. EX-1041, [0003] ("It is known to configure the mobile device with the WAP gateway address and WAP port number via the user interface of the mobile

device.… In OTA programming, ***the service provider can transmit an SMS configuration message*** to the mobile device whereupon the mobile device configures itself with the WAP gateway address and port number included in the SMS configuration message."); EX-1042, [0032] ("The one or more databases 134 may comprise one or more entities that contain user related information such as subscription and configuration (e.g. user profile, subscription, operator services, Home Location Register ('HLR'), etc.) and provide customized processing instructions. The one or more databases 134 may provide MMS user subscription information, information for the control of access to the MMS, information for the control of the extent of available service capability (e.g. server storage space), a set of rules how to handle incoming messages and their delivery, and information of the current capabilities of the user's terminal."); EX-1057, [0032] ("The MM preferably ***manages a user database and contains the update status of each one of the endpoints 156/166*** as well as their connection parameters and capabilities."); EX-1058, [0043] ("the wireless service provider [may] update the relevant database so that the user's MSISDN number points to the address of the MMS server belonging to the ISP."); EX-1059, [0037] ("the respective recipient rules can be uploaded or otherwise transferred to the respective databases for storage. For example, the recipients can transmit the recipient rules to the profile

server, which thereafter stores the recipient rules in the database associated with the profile server.”).

163. Based on TS-23.140’s disclosures and as corroborated by contemporaneous references discussing MMS, a POSA understood TS-23.140 to teach a User Agent device comprising a hardware/software element (the claimed “policy control agent”) that receives and processes user-subscription and configuration information (“message content” in a “first format that contains service settings and/or configuration information”). TS-23.140 expressly says that such user-subscription/configuration processing and similar functionality need not be performed by its MMS User Agents. EX-1004, 19 (listing “user profile management” as an ***optional*** function for the MMS User Agent). In view of this disclosure, a POSA would have recognized that implementing MMS-Rakic’s “policy control agent” as a separate, dedicated element (e.g., a software component, such as an application) that communicates with MMS-Rakic’s User Agent (“device link agent”) over MMS-Rakic’s “inter-process software communication bus” was a viable implementation option.

164. A POSA further would have recognized such an option as desirable because it would have simplified MMS-Rakic’s User Agent functionality and permitted an implementation where the User Agent’s functions were focused on primarily handling processing and delivery of MMs (e.g., to destination

applications)—functions which are logically distinct from user profile and policy control management. A POSA understood that implementing MMS-Rakic's "policy control agent" as a separate, dedicated element would also provide the advantages of (1) allowing the policy control logic to be used as a common service by other communication interfaces (e.g., email, SMS, or other data services) or applications on the device, and (2) providing update flexibility by allowing updates to the policy control logic without requiring changes to the User Agent. Likewise, based on TS-23.140's disclosure of such user-subscription/configuration processing and similar functionality as only ***optionally*** handled by the MMS User Agent, and further based on my understanding of a POSA's skill as discussed in Section IV above, a POSA would have reasonably expected success with such an implementation, which would have been well within a POSA's ability to implement. Such an implementation would have met claim 6's requirement of a "first device component" that "is a policy control agent," and "first format" that "contains service settings and/or configuration information."

7. Claim 7: The mobile end-user device of claim 1, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes.

165. Claim 7 requires "the received secure messages" to be "encrypted," and "the device link agent" to be "configured to decrypt the received secure messages prior to delivering those messages to respective software processes."

166. As I discussed above in Section VII.D.1.h.i, "received secure messages" are "secure[d]" using SSL/TLS (as I discussed above in Section VII.C.2), and signed and encrypted pursuant to Rakic's teachings. EX-1007, [0075] (disclosing messages secured using "a combination of generating a signature ***and encrypting the data***" in the payload), [0078] ("Data field 822 may include content (e.g., payload)"). See also my discussion above in Section VII.B. SSL/TLS is a form of encryption. Therefore, a POSA understood that "the received secure messages are encrypted," as claimed.

167. TS-23.140 expressly identifies the MMS User Agent as "provid[ing]… functionalities such as… decryption and encryption of an MM on an end-user to end-user basis." EX-1004, 19. Moreover, a POSA understood that decrypting received secure messages at the endpoint of MM1 in MMS-Rakic—the MMS User Agent on the user device—would have desirably facilitated, e.g., decrypting the necessary information to validate and then accurately routing,

within the device, the application data being transported by the MMS User Agent, as I discussed above in Section VII.D.1.i. *See* EX-1004, 54-56 ("the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier"). A POSA thus understood that the MMS User Agent is "configured to decrypt the received secure messages prior to delivering those messages to respective software processes," as claimed.

8. Claim 8: The mobile end-user device of claim 7, wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.

168. Claim 8 recites a list of alternatives ("one or more of") for transporting the claimed "messages" to the device messaging agent, including "encryption on a transport services stack." As I discussed above in Section VII.D.1.c.i, in the '564 specification, external communication with the component that "provid[es] the device side of a system for transmission and reception" of messages (i.e., "service control device link 1691"), occurs over "service control link 1653." EX-1001, 38:5-8, 69:25-34. The '564 specification describes including a "layer[] of encryption in the service control link" that is "***implemented in the transport services stack (2410, 2420)***" using "***standard secure or open Internet networking protocols, such as TLS or TCP***." EX-1001, 89:14-36. As I discussed

above in Section VII.C.2, MMS-Rakic's MM1 utilizes TLS. This TLS protocol provides secure data transmission between the MMS User Agent and the MMS Relay/Server "in architectural configurations that employ HTTP based protocol stacks" or WAP protocol stacks via the transport services stack layer. EX-1012, 21. The MM1 interface using TLS thus provides encryption at the transport services stack layer. A POSA thus understood that, just as in the '564 specification, MMS-Rakic's use of the SSL/TLS protocol to secure the MM1 interface is implemented in a transport services stack, and is "***encryption on a transport services stack***," as claimed.

9. Claim 10: The mobile end-user device of claim 1, wherein the device link agent is further configured to receive, from one or more of the authorized software components, upload messages, each of the upload messages identifying a corresponding one of the network functions to which the device respective software component has requested delivery, the device link agent transmitting the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements.

169. Claim 10 requires that the "device link agent" is "configured to receive" "upload messages" "from one or more of the authorized software components." The "upload messages identify[] a corresponding" "network function[] to which" the "software component has requested delivery." Claim 10 says the "device link agent transmit[s] the upload messages to the network

message server over the secure message link, for delivery by the network message server to the respective identified network elements."

170. "Network message server" has no antecedent basis; the only recited server the "device link agent maintain[s] a secure message link" to is claim 1's "message link server." Likewise, "network elements" has no antecedent basis; the only element "identified" in the "upload messages" are "network functions." A POSA thus understood that Claim 10 at minimum encompasses an interpretation where the recited "network message server" is claim 1's "message link server," and the recited "respective identified network elements" are the "corresponding… network functions" identified in claim 10's "upload messages."

171. As I discussed above in Sections VII.A and VII.D.1.c.i-VII.D.1.c.ii, MMS is used to transport application-specific data between MMS VAS Applications and applications on a user device (other than the MMS User Agent). EX-1004, 14, 54-55. As I discussed above in Section VII.D.1.d, in MMS-Rakic, a MMS User Agent receives, via the MMS Relay/Server, a message from a MMS VAS Application that contains "access authorization information"—comprising a signature and a destination application identifier—which the MMS User Agent validates and uses for routing the message to the identified destination application over a bus. A POSA understood that such destination applications are "authorized software components," as claimed, because they are the destination applications

identified in validated messages and thereby authorized to receive messages over MMS-Rakic's bus.

172. As I discussed above in Sections VII.D.1.h-VII.D.1.i, MMS-Rakic's MMS User Agent (the claimed "device link agent") exchanges "secure messages" containing application-specific data with MMS-Rakic's MMS Relay/Server over the "secure message link" (MM1). These messages go ***both ways***—MMS can also be used to ***upload*** messages from the user device to a VASP (via the MMS Relay/Server). TS-23.140 expressly discloses MMS being "used to transport data specific to applications between… an MMS User Agent and an MMS VAS Application (***or vice versa***)" (EX-1004, 55)—for example, an "abstract message[]… sent ***by an MMS User Agent… on behalf of an originating application***" on the user device (*id.*) that is "passed by the MMS Relay/Server ***to a VASP***" (EX-1004, 116-117, FIG. 9). An example of this would be, e.g., an application on the device for chess using MMS to transport data regarding a user's inputted chess move to a chess VAS Application.

173. TS-23.140 discloses that "an application may trigger an MMS User Agent… to submit" "abstract messages." EX-1004, 55. "Upon" this "triggering" by an application to send an abstract message—the MMS User Agent "insert[s]" information "receive[d]… from the application" into an "abstract message" and

sends it. *Id.* Because the originating device application[4] triggers the MMS User Agent to send an abstract message that incorporates information provided by that application, a POSA understood that MMS-Rakic's User Agent is "configured to receive" "upload messages" containing this information from claim 1's "software components." A POSA understood that MMS-Rakic's "upload messages" are then packaged as abstract messages comprising a destination application identifier and content for delivery to the VASP, and sent to the MMS Relay/Server over MM1. EX-1004, 55 ("The MMS User Agent… may insert… information" "from the application" in both the information elements and/or payload… of the abstract message."), 62-63 (describing the sending of a MM by a MMS User Agent that "shall be provided to an application residing on an… MMS VAS Application" using a MM1_submit.REQ abstract message), 65 (MM1_submit.REQ messages contain Applic-ID and Content elements), 116-118 (describing the sending of a MM that "originated from the MMS User-Agent," by the MMS Relay/Server to a MMS VAS Application using a MM7_deliver.REQ abstract message).

[4] In the context of claim 1, this application is called the destination application to which application-specific data is transported, as I discussed above in Section VII.D.1.c.ii.

174. As explained in paragraphs 175-178 below, TS-23.140 illustrates how such information is transmitted to the VASP (via the MMS Relay/Server) using its MM1_submit.REQ and MM7_deliver.REQ "abstract message" examples. *See* EX-1004, 62, 116, 58, 189-190. Specifically, as explained in paragraphs 175-178 below, TS-23.140 discloses how the MM1_submit.REQ message information from the MMS User Agent is sent by the MMS Relay/Server via an MM7_deliver.REQ message to the VAS Application.

175. TS-23.140 describes the MM1_submit.REQ "abstract message" in Table 4, copied below. EX-1004, 62 (Table 4).

Table 4: Abstract messages for submission of MM in MMS

Abstract messages	Type	Direction
MM1_submit.REQ	Request	MMS UA -> MMS Relay/Server
MM1_submit.RES	Response	MMS Relay/Server -> MMS UA

176. "The MMS Relay/Server will deliver messages to the VASP by supplying the MM as the payload of the MM7_deliver.REQ. The message originates, for example, from a MMS User Agent, an external application, or from outside the MMSE. This delivery may include an identification of the request that may be used by the VASP to correlate a response to the message." EX-1004, 116-117. TS-23.140 describes the MM7_deliver.REQ "abstract message" in Table 61, copied below. EX-1004, 116 (Table 61).

Table 61: Abstract messages for demanding a service from a VASP

Abstract messages	Type	Direction
MM7_deliver.REQ	Request	MMS Relay/Server -> VASP
MM7_deliver.RES	Response	VASP -> MMS Relay/Server

177. "The MMS Relay/Server shall translate recipient addresses that originate from the MM1 interface into the appropriate URL of the VASP, for example ***when an MM7_deliver.REQ results from an MM1_submit.REQ from the MMS User Agent***." EX-1004, 58 (Section 7.2.3); *see also* EX-1004, 189-190 (Annex K; mapping information elements in the MM1_Submit.REQ abstract message to information elements in the MM7_Deliver.REQ abstract message in Table K.1, including Applic-ID and Content; "There is a table for each MM1… abstract message that maps to a MM7 abstract message.").

178. TS-23.140 discloses that, after the MMS Relay/Server receives an MM1_submit.REQ message from the MMS User Agent, it sends an MM7_deliver.REQ message to the MMS VAS Applications server. EX-1004, 116-117 ("The MMS Relay/Server will deliver messages" that "originate[]… from a MMS User Agent" "to the VASP by supplying the MM as the payload of the MM7_deliver.REQ[.]"), FIG. 9 (annotated below):

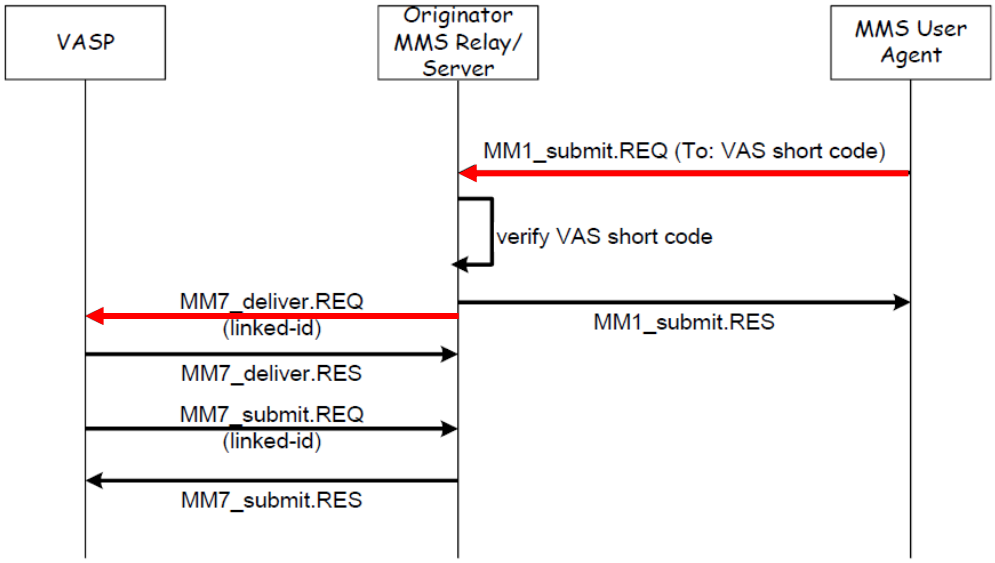


Figure 9: Use of MM7_deliver and subsequent response

EX-1004, 117, FIG. 9 (annotated)

179. Claim 10 requires that "each of the upload messages identify[] a corresponding one of the network functions to which the device respective software component has requested delivery." In MMS-Rakic, the "abstract message" sent to the Relay/Server "shall contain a destination application identifier" for use by the VAS Application to "immediately route the received MMS information on to the destination application that is referred to by the destination application identifier." EX-1004, 55-56; *see also id.*, 63 ("The presence of this information element indicates that this abstract message shall be provided to an application residing on an… MMS VAS Application. It contains the identification of the destination application" and "MM recipients of a submitted

MM shall be indicated in the addressing-relevant information field(s) of the MM1_submit.REQ"), 65 (same), 117-118 (The "Applic-ID… information element [of a MM7_Deliver.REQ message] contains the identification of the destination application. Upon reception, the recipient MMS VAS Application shall provide [the message] to the specified destination application" and "[a]ll relevant address information for the delivery of the message to the VASP… should be included in the relevant information elements of MM7_deliver.REQ.").

180. A POSA therefore understood that the claimed "upload message" that MMS-Rakic's MMS User Agent receives from a destination application (which, as I explained above in paragraph 173, the MMS User Agent the packages as an "abstract message" to send to the MMS Relay/Server) includes information "identifying a corresponding one of the network functions" to which delivery of the message is requested—because that information allows the MMS User Agent to include the destination application identifier that the VAS Application uses to route the message to the correct destination application. EX-1004, 55-56.

181. Claim 10 further requires that "the device link agent transmit[] the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements." A POSA understood that MMS-Rakic does this. As I explained above in paragraphs 174-178 (citing EX-1004, 58, 62, 116, 189-190), TS-23.140

illustrates how information from a device application is transmitted to a VASP (via the MMS Relay/Server) using its MM1_submit.REQ and MM7_deliver.REQ "abstract message" examples. TS-23.140 discloses that after the Relay/Server receives an MM1_submit.REQ message from the User Agent, it sends an MM7_deliver.REQ message to the VAS Application. EX-1004, 116-117 ("The MMS Relay/Server will deliver messages" that "originate[]… from a MMS User Agent" "to the VASP by supplying the MM as the payload of the MM7_deliver.REQ[.]"), FIG. 9 (annotated below):

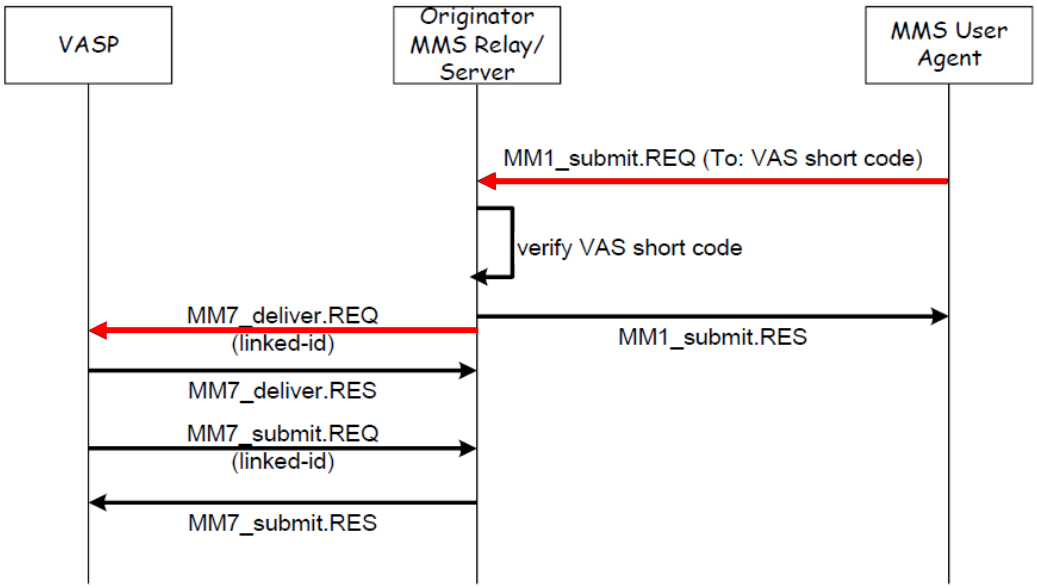


Figure 9: Use of MM7_deliver and subsequent response

EX-1004, 117, FIG. 9 (annotated)

182. MMS-Rakic's User Agent (the claimed "***device link agent***," as I discussed above in Section VII.D.1.c.i) thus "***transmit[s] the upload messages to***

the" MMS Relay/Server (the claimed "message link server," as I discussed above in Section VII.D.1.f, which claim 10's "***network message server***" encompasses) "***over the secure message link***" (MMS-Rakic's MM1, as I discussed above in Section VII.D.1.f), "***for delivery by the"*** MMS Relay/Server "***to the respective identified***" MMS VAS Applications (the claimed "network functions," as I discussed above in Section VII.D.1.g, which claim 10's "***network elements***" encompass).

10. Claim 12: The mobile end-user device of claim 1, wherein at least one of the secure messages received from the network message server comprises multiple identifier/data pairs.

183. Claim 12 recites "at least one of the secure messages received from the network message server comprises multiple identifier/data pairs." As I discussed above in Section VII.D.9, "network message server" has no antecedent basis and at minimum encompasses claim 1's "message link server."

184. The '564 specification does not describe a "secure message" that "comprises multiple identifier/***data*** pairs." During prosecution of related U.S. Patent No. 9,232,403, which shares a specification with the '564 Patent, PO identified "Figure 25 [as] illustrat[ing] such a… message structure, wherein… the data message… ***is composed of*** [multiple] agent ***messages***, each formatted as an agent identifier with a paired message payload[.]" EX-1060, 736. FIG. 25 (annotated below) shows a "service controller communication ***frame***" comprising

multiple identifier/***message*** pairs (respectively blue, green). EX-1001, 91:11-63 (describing FIG. 25).

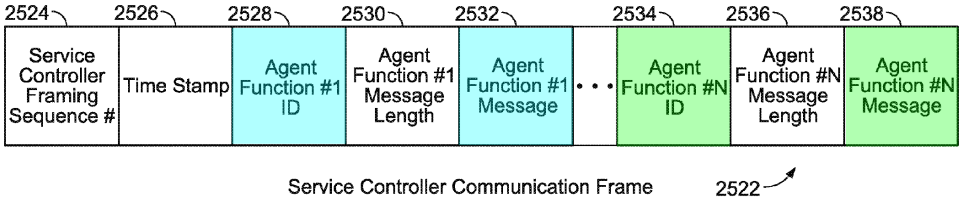


FIG. 25

EX-1001, Fig. 25 (annotated)

185. Additionally, the ’564 specification states that “service control server link 1638 can perform collection or buffering of server messages between transmissions[, and] once a transmission trigger has occurred, …take all buffered agent communications and frame the communications.” EX-1001, 70:3-16. PO’s prosecution statements (for the “multiple identifier/data pairs” limitation during prosecution of the ’403 patent, EX-1060, 736) indicate that claim 12’s “message[] compris[ing] multiple identifier/data pairs” thus encompasses a network message server that collects and buffers messages (each comprising an agent identifier and payload), and then sends the collected messages to a “device messaging agent” as a group or frame of messages.

186. TS-23.140 describes, upon receiving a message, the MMS Relay/Server “stor[ing] the MM at least until: the associated time of expiry is reached, the MM is delivered, the recipient MMS User Agent requests the MM to be routed forward, [or] the MM is rejected.” EX-1004, 28; *see generally id.,* 26-28

(Sections 7.1.1-7.1.2, Submission and Reception of Multimedia Messages). Messages may be "persistent[ly] stored" (EX-1004, 21) in a "Persistent Network-Based Storage" (MMBox) associated with "the MMS Relay/Server." EX-1004, 22 (Section 5.2.1, Persistent Network-based Storage (MMBoxes)), 26-28 (Sections 7.1.1-7.1.2, Submission and Reception of Multimedia Messages).

187. When an unavailable recipient MMS User Agent becomes available, e.g., by moving into coverage, the MMS Relay/Server delivers the group of collected messages to the MMS User Agent. EX-1004, 29 (Section 7.1.3, Retrieval of a Multimedia Message in the recipient MMSE). As I explained above in Section VII.D.1.h, each message in the group of abstract messages comprises a destination application identifier and application data. The group of collected messages delivered to the MMS User Agent is thus a "secure message[] received from the network message server compris[ing] multiple identifier/data pairs," as claimed.

188. Further, aggregating multiple messages in a single frame would have been obvious. A POSA had reason to implement MMS-Rakic such that the MMS Relay/Server transmits multiple collected MMs to a MMS User Agent in a frame comprising multiple MMs. TS-23.140 is part of a broader 3GPP suite of specifications—well-documented and well-known to a POSA, as discussed below—that define layered architecture and data transport mechanisms for MMS communications over 3G packet-switched bearers.

189. TS-23.140 contemplates each MM being conveyed in an HTTP message over TCP/IP, which is delivered to the radio access network through the 3G packet-switched bearer service. EX-1021 (MMS Encapsulation Protocol), 11, 13, 48 (incorporated into EX-1004 at 12, 174-175). Moreover, a POSA would have understood that multiple higher-layer data units—e.g., multiple HTTP messages, each carrying a distinct MM—would be aggregated within a single lower-layer frame for transmission to a MMS User Agent. Under the Release 6 bearer architecture, those same HTTP/TCP data units are carried by the Packet Data Convergence Protocol (PDCP, 3GPP TS 25.323), the Radio Link Control (RLC, 3GPP TS 25.322), and the Medium Access Control (MAC, 3GPP TS 25.321). The RLC layer in particular is expressly permitted to segment and/or concatenate multiple service data units to form a single protocol data unit for transmission, while the MAC layer multiplexes multiple RLC PDUs within a single transport block. *See*, *e.g.,* TS-25.323 (PDCP) (EX-1053), 8-9, 23 (explaining PDCP performs transfer of upper-layer PDUs, e.g., MMS/HTTP/TCP/IP, containing user data, and "uses the services provided by the [RLC] sublayer"); TS-25.322 (RLC) (EX-1052), 11, 16, 22-23 (explaining RLC concatenates RLC SDUs (e.g., PLDC PDUs) into PDUs for the MAC layer); and TS-25.321 (MAC) (EX-1051), 12, 15, 28-29, 46-47 (explaining RLC PDUs are provided to the MAC layer, and concatenated into MAC PDUs before transmission). This was desirable because

encapsulating multiple identifier/data pairs, or multiple MMs, within a single frame would improve radio-interface efficiency and reduce protocol overhead.

190. Moreover, a POSA would have reasonably expected success implementing MMS-Rakic's MMS Relay/Server to transmit a group of messages using such a frame, especially considering the relevant 3GPP specifications (see my discussion above in paragraph 189) that expressly support encapsulation of multiple higher-layer data units into a single transport block for precisely this reason.

191. Thus, implementing MMS-Rakic such that the MMS User Agent receives a message (e.g., a frame) containing "multiple ID/data pairs" was obvious.

11. Claim 13: The mobile end-user device of claim 2, wherein the given one of the software components is identified by a secure unique identifier.

192. Claim 13 requires that claim 2's "given one of the software components is identified by a secure unique identifier." As I discussed above in Sections VII.D.1.d, VII.C.4, and VII.D.2, the "given one of the software components" of claim 2 is "identified by… access authorization information" comprising a signature and a destination application identifier that identifies the destination application. A POSA understood that the identifier ***uniquely*** identifies the destination application. EX-1004, 55 (describing ways to "guarantee… global uniqueness"). And, as I discussed above in Sections VII.C.4, VII.D.1.d, and

VII.D.1.h.i, a POSA understood that the destination application identifier is part of a secure message that is (1) signed by the signature, (2) encrypted per Rakic's teachings, and (3) sent over MM1 which is secured using SSL/TLS (as I discussed in Section VII.C.2 above). A POSA thus understood that MMS-Rakic's destination application is "identified by a ***secure*** unique identifier," as claimed.

12. Claim 14

193. Claim 14 recites a "method of operating a mobile end-user device" that recites steps corresponding to system limitations recited in claim 1. MMS-Rakic meets each element of claim 14 for the same reasons I discussed above for the corresponding element in claim 1, as summarized in the table below:

Claim 14 Elements	Corresponding Claim 1 Elements	Section
[14PRE]	[1PRE], [1A]	§§VII.D.1.a-b
[14A]	[1B2]	§VII.D.1.d
[14B1]	[1B1]	§VII.D.1.c
[14B2]	[1B2]	§VII.D.1.d
[14C1]	[1D1]	§VII.D.1.f
[14C2]	[1D2]	§VII.D.1.g
[14D]	[1E]	§VII.D.1.h
[14E]	[1F]	§VII.D.1.i

VIII. GROUNDS 2A-2C

194. I note that in IPR2024-00341, the Board previously agreed that it would have been obvious to implement TS-23.140 with a modem for network communications (as I discussed above in Section VII.C.1) and a software bus (e.g.,

a D-bus) for interprocess communications (as I discussed above in Section VII.C.3). EX-1022, 40-41, 45, 48-49.

195. As I discuss below in Grounds 2A-2C, a POSA would have also alternatively been motivated to modify the combination of TS-23.140 and Rakic that I describe above in Ground 1 in view of (1) express teachings in Cole (of a modem, which I discuss below as Ground 2A), (2) express teachings in Sathish (of an interprocess communication bus, which I discuss below as Ground 2B), and (3) ***both*** Cole and Sathish (which I discuss below as Ground 2C).

A. GROUND 2A: MMS-Rakic in View of Cole (EX-1006)

196. As I discussed above in Section VII.C.1 (e.g., paragraphs 60 and 62), it was well-documented before the Critical Date to use a ***modem*** to enable communications over the 2G/3G WWAN networks described in TS-23.140. For example, for connecting a "mobile device" to a "2G"/"3G" "wireless wide area network (WWAN)"—which "may interface directly or indirectly with a public network (e.g., the Internet)"—Cole expressly discloses implementing the mobile device's various "communication interfaces" to include "***a WWAN modem***." EX-1006, [0031] (describing a "mobile device" that interfaces with a "plurality of communication networks" including 2G and 3G wireless cellular technologies), [0034]-[0035] (describing interfacing with Cole's disclosed networks using a

communication interface that includes "a WWAN modem"), [0003] (discussing "wireless connection[s] to the Internet"), FIGS. 1-2 (illustrating same, below).

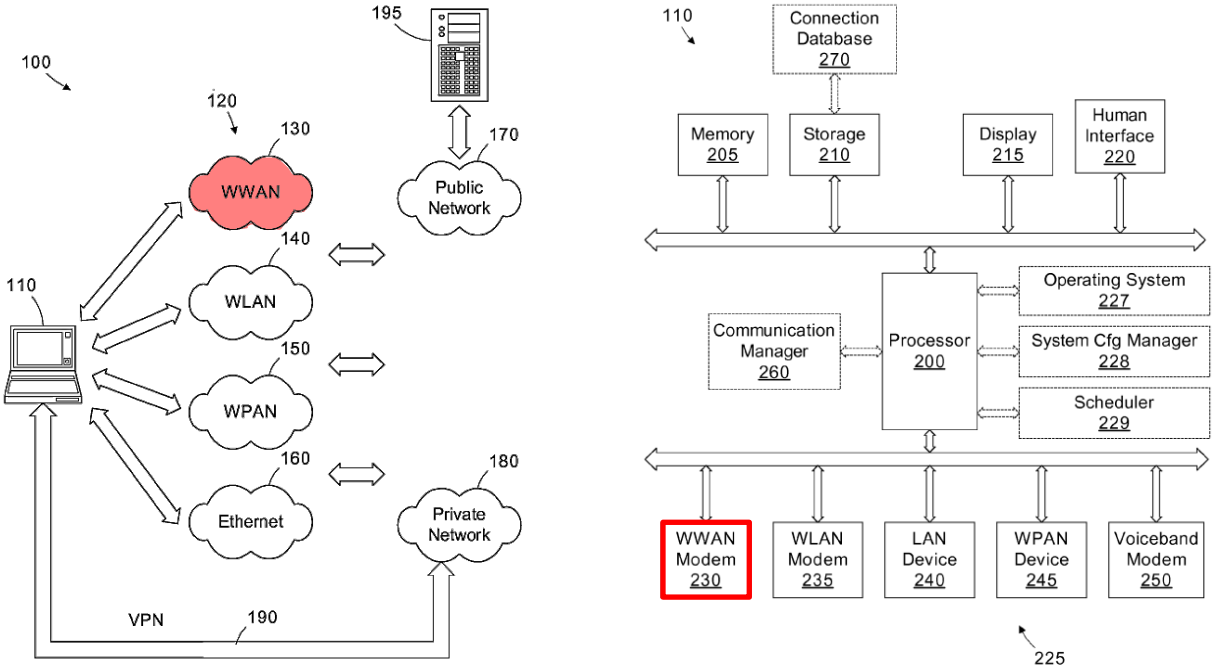


Figure 1 **Figure 2**

EX-1006, FIGS. 1-2 (annotated)

Cole confirms that "[t]he various protocols required to implement connections over [such] communication interfaces… to [such]… communication networks… ***are known to those [of] ordinary skill***." EX-1006, [0035].

197. In view of Cole, (e.g., the teachings I discuss above in paragraph 196 from EX-1006, [0003], [0031]-[0035], FIGS. 1-2), a POSA would have been motivated to use a "WWAN ***modem***" to enable TS-23.140's user device to communicate over TS-23.140's disclosed 2G/3G wireless networks, and would have reasonably expected success doing so. Such an implementation would have

been nothing more than using familiar, known components (Cole's WWAN modem in TS-23.140's user device that communicates over 2G/3G networks) to achieve a predictable result of facilitating TS-23.140's disclosed communications.

198. This combination renders obvious claims 1-8, 10, and 12-14 for the same reasons, respectively, I discussed above in Section VII for MMS-Rakic.

B. GROUND 2B: MMS-Rakic in View of Sathish (EX-1031)

199. As I discussed above in Section VII.C.3, it was well-documented before the Critical Date to use a software ***bus*** to enable the interprocess communications described in TS-23.140. EX-1004, 14, 54-56; EX-1028, 729-730, 732-733, FIGS. 4-5. For example, Sathish describes a "D-Bus" as "an example of a device inter-process communication channel used to send information between applications." EX-1031, 10:56-62.

200. In view of Sathish, a POSA would have been motivated to implement the interface between TS-23.140's MMS User Agent and the user device's other applications using a software bus, e.g. D-Bus, and would have reasonably expected success doing so. Using such a bus to enable TS-23.140's applications to interface would have been nothing more than using familiar, known components to achieve a predictable result of facilitating TS-23.140's communications. For additional documentary evidence corroborating this teaching, *see also* EX-1048, [0001], [0003], [0004], [0019] (describing "communication" between "one or more

processes" occurring over a "bus"); EX-1049, 907 (defining "software bus": "A programming interface that allows software modules to transfer data to each other…"); EX-1050, 2:64-3:6 (describing "software bus" that "interconnects" a "control software's subsystems"), 3:51-67, FIG. 5.

201. This combination ("MMS-Rakic-Sathish"), with the bus providing secure communications in the manner I discussed above in Section VII.C.4, renders obvious claims 1-8, 10, and 12-14 for the same reasons, respectively, I discussed above in Section VII for MMS-Rakic.

C. GROUND 2C: MMS-Rakic-Cole-Sathish

202. A POSA understood that the modifications I describe above in Sections VIII.A and VIII.B are compatible with each other. Moreover, it was feasible and desirable to implement MMS-Rakic's device to incorporate the WWAN modem in view of Cole (for the reasons I discussed above in Section VIII.A) **and** a software interprocess communications bus in view of Sathish (for the reasons I discussed above in Section VIII.B). Such a combination (MMS-Rakic-Cole-Sathish) renders obvious claims 1-8, 10, and 12-14 for the same reasons, respectively, I discussed above in Section VII.

IX. GROUNDS 3A-3D

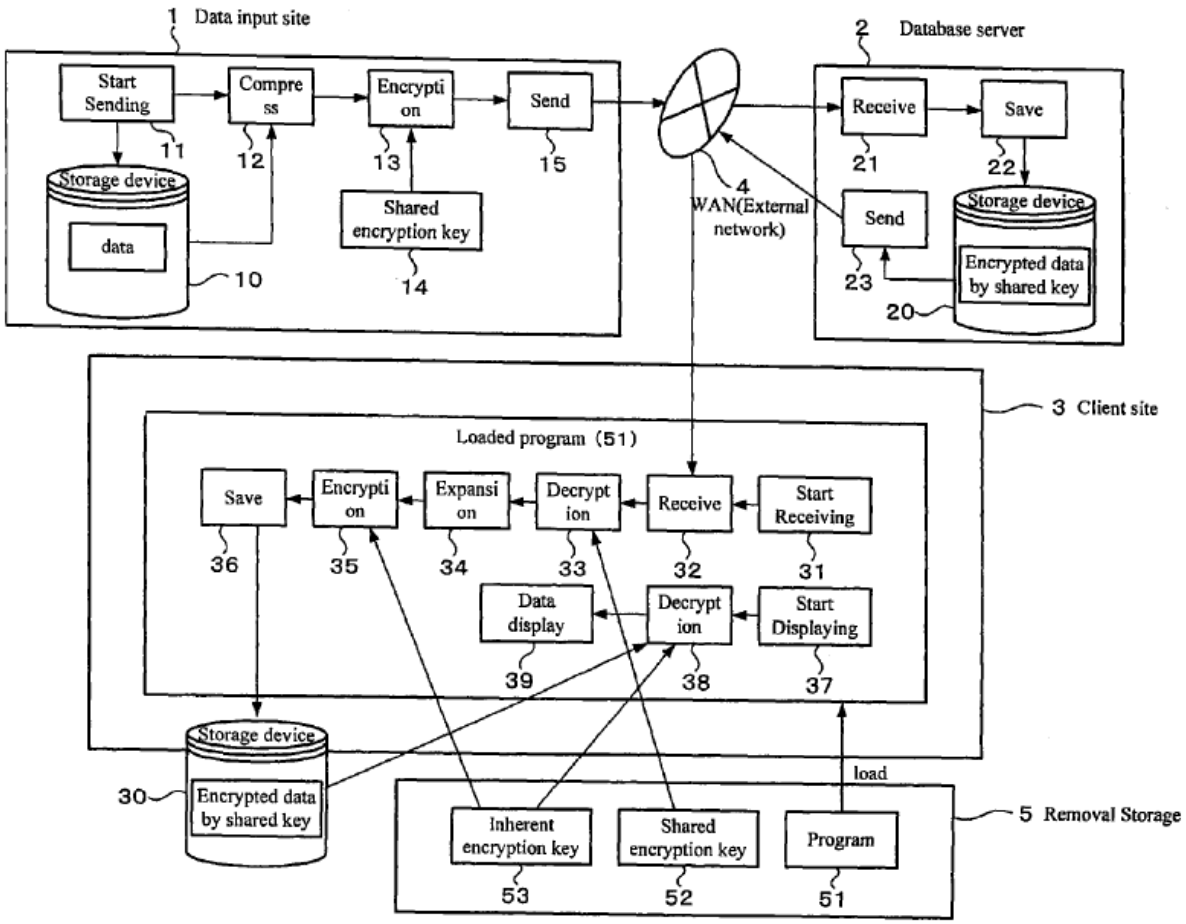
203. As I discussed above in Section VII.D.7, MMS-Rakic's meets claim 7, at least because the secure messages received by MMS-Rakic's user device are

encrypted, and MMS-Rakic's MMS User Agent is "configured to decrypt the received secure messages prior to delivering those messages to respective software processes." However, to the extent claim 7's "encrypt[ion]"-related requirements are not considered rendered obvious over MMS-Rakic, a POSA understood that they are rendered obvious by incorporating Ogawa's (EX-1005) teachings.

A. Ogawa (EX-1005)

204. Ogawa discloses a "data encryption system" (EX-1005, 3:18-21), an example of which is shown below:

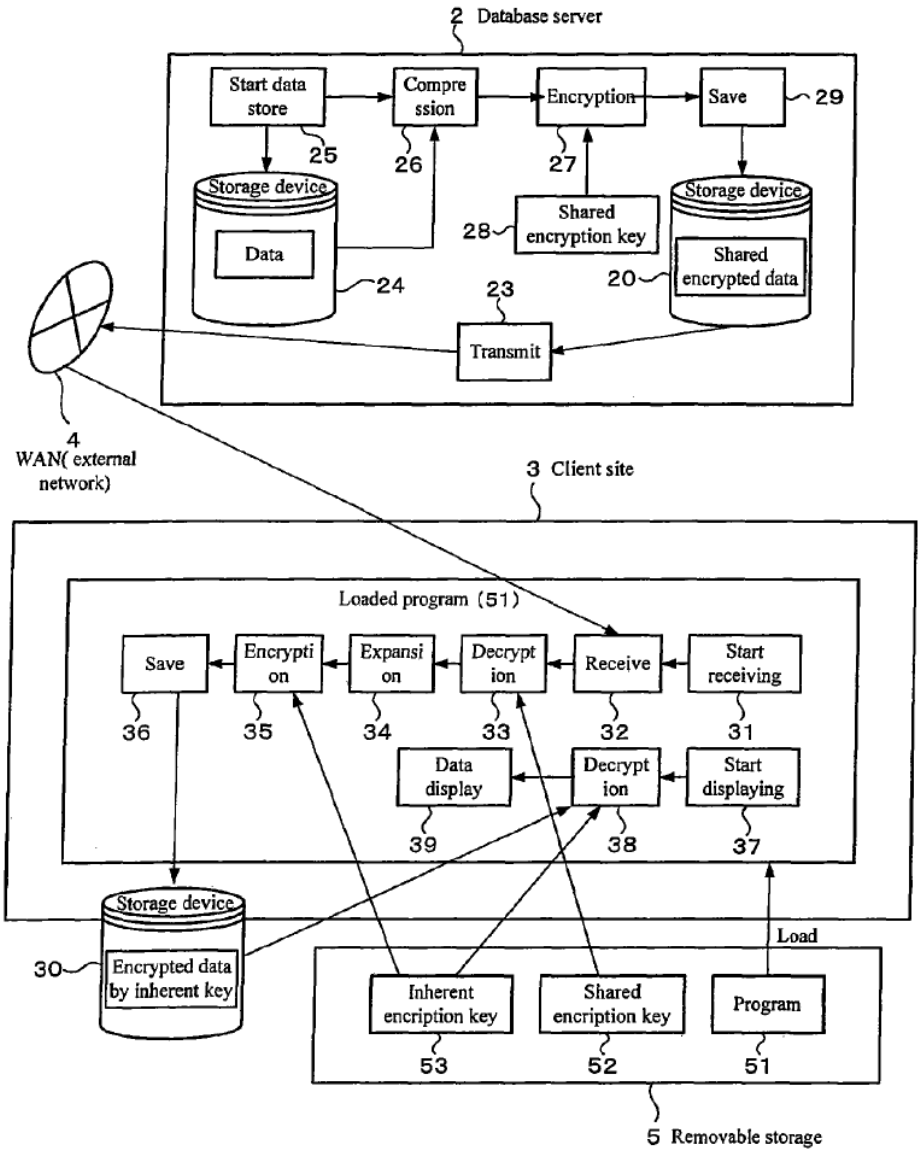
Figure 1



EX-1005, FIG. 1

With reference to FIG. 1, Ogawa's system facilitates communications between multiple entities, including: (i) data input site 1, (ii) database server 2, and (iii) client site 3. These entities are "operably linked via an external wide area telecommunication network 4," for example, "the Internet" supported by "hyper text transfer protocol (HTTP)." EX-1005, 3:44-54 (describing FIG. 1).

205. Ogawa discloses several configurations for its system that facilitates secure communications between a database server and a client site through a network. *E.g.,* EX-1005, 9:15-38 ("… FIG. 7 shows the block configuration of an exemplary system in which the database server 2 is integrated with the function of a data input site 1 and the database server 2 and the client site 3 are connected through the external network 4."), FIG. 7 (below). For example, FIG. 7 (below) illustrates a client-server system that performs functions described for FIG. 1 (described further below):



EX-1005, FIG. 7

In the system shown in FIG. 7, "the database server 2 is integrated with the function of a data input site 1" and "the database server 2 and the client site 3 are connected through the external network 4." EX-1005, 9:16-20; *see generally id.,* 9:15-38 (describing FIG. 7).

206. Ogawa uses security protocols for data transmission between network entities, e.g., between a client computer and a server. "For example, in network communications using a conventional TCP/IP (Transmission Control Protocol/Internet Protocol) or UDP (User Datagram Protocol), ***encryption communication, such as*** IPsec (Internet Protocol Security) or SSL (Secure Socket Layer), is utilized to prevent some security risks presented during the exchange of data between network terminals." EX-1005, 3:64-4:4. A POSA understood that SSL was known as a predecessor of TLS, and thus, a POSA understood that TS-23.140, Rakic, and Ogawa contemplated similar secure data transport within their networks. For documentary evidence corroborating my testimony, *see, e.g.*, EX-1010, 1:38-42 ("[T]he Secure Socket layer (SSL) protocol and its successor Transport Layer Security (TLS) provides a mechanism for securely sending data between a server and a client.").

207. Ogawa teaches ***further*** securing data by, for example, using a "shared encryption key" used by client and server. EX-1005, 6:42-47 (describing "operations that distribute… shared encryption keys"), 7:11-21 (describing transmission and storage of encryption keys), 9:16-38 (describing use of "shared encryption key 28" in FIG. 7).

208. The shared key referenced above is used to (1) encrypt data that is transmitted as encrypted data to the client from the server (as discussed above),

and (2) decrypt received encrypted data at the client. EX-1005, 9:21-34 (compress, encrypt, store data), 5:60-65 (decrypt) . For example, Ogawa teaches that at client site 3, the encrypted data is received by the receive unit 32 and this encrypted data is decrypted by decryption unit 33 using a shared encryption key 52. EX-1005, 5:59-67, 7:11-21. The shared encryption key is stored in storage (e.g., a removable storage 5) and is provided to decryption unit 33 to perform the decryption. *Id*.

209. The shared encryption key is distributed to both data input site 1 and client site 3. EX-1005, 6:42-45. Once client site 3 has the key, "the client site 3 will send the encryption key to the removable storage 5," which is "is operably linked to the client site 3 (physically or wirelessly)…." EX-1005, 6:46-47, 7:16-21. "When the removable storage 5 receives the encryption key from the client site 3[,] it stores the encryption key into the memory device in the removable storage…." EX-1005, 7:18-21.

B. GROUND 3A: Implementing Ogawa's Encryption Teachings

1. MMS-Rakic-Ogawa

a. Applying Ogawa's Symmetric Encryption Techniques

210. TS-23.140 discloses "encryption of an MM [Multimedia Message] on an end-user to end-user basis." EX-1004, 19. In addition to "transport layer security mechanisms," TS-23.140 says "authentication mechanisms based on public/private key cryptography… may ***also*** be used." EX-1004, 25, 41; EX-1012,

21 ("An aspect of the MMS user interface is that of conveying information related to the security and/or authentication of messages received or to be sent."). For example, Public Key Infrastructure (PKI) is one security service that may be implemented via MM1 using WAP/OMA. EX-1004, 30 (WAP/OMA implementation), 41 (7.1.13.1 Authentication); EX-1012, 21 (PKI as example of "security services"). Moreover, as I discussed above in Section VII.B, Rakic discloses "perform[ing] a combination of generating a signature ***and encrypting the data***" when securing messages. EX-1007, [0075] (disclosing messages secured using "a combination of generating a signature ***and encrypting the data***" in the payload), [0078] ("Data field 822 may include content (e.g., payload)").

211. A POSA understood that "an end-user" can be an MMS User Agent, or an MMS Relay/Server. *See e.g.*, EX-1004, 62 ("Reference point MM1 defines the transactions between the MMS User Agent and the MMS Relay/Server.… Figure 6 illustrates some of these transactions and their relationships, in an ***end-to-end*** manner."). Alternatively, it would have been obvious to a POSA to ensure a message (being sent between end-users via the MMS Relay/Server) is encrypted when it is stored on the MMS Relay/Server and sent from the MMS Relay/Server to the receiving MMS User Agent. *See* EX-1004, 17 ("The MMS Relay/Server is responsible for storage and handling of incoming and outgoing messages and for the transfer of messages between different messaging systems."). A POSA would

have been motivated to do so, for example, to make sure a message received at the MMS Relay/Server would be secure from, *e.g.*, theft, access, or manipulation while stored there and when sent to the MMS User Agent. *See e.g.*, EX-1005, 8:16-21 (disclosing encryption of a message before storing it).

212. Neither TS-23.140 nor Rakic provides details regarding how to implement the additional end-user-to-end-user encryption beyond SSL/TLS. However, before the Critical Date, it was well-known and well-documented to implement encryption for messages transmitted by a server (*e.g.,* TS-23.140's MMS Relay/Server) to an end-user device using symmetric encryption, with a key that is shared between the server and the end-user device and stored in the respective memories. Multiple references before the Critical Date disclose encryption solutions where the data in messages sent between server and a client is encrypted using a shared key stored by the client and server, and the shared key is used for encrypting/decrypting messages sent between the client and the server. For example, Shen (EX-1027) discloses data encryption over push messages (MMS messages) using a shared key established by the client and server and distributed to users, and using this shared key for encrypting/decrypting messages between user devices. EX-1027, [0054]-[0060]. Another example is Qumei (EX-1009). *See*, *e.g.*, EX-1009, 3:25-27 ("[A]n enciphering algorithm and an enciphering key may be stored in the electronic devices"), 8:1-5 ("Symmetric

cyphering/enciphering may use one or multiple keys for both encryption and decryption"). Another example is Rakic itself. EX-1007, [0075] (disclosing messages secured using "a combination of generating a signature ***and encrypting the data***" in the payload). And Ogawa (EX-1005), discussed above in Section IX.A, discloses details regarding how to implement symmetric encryption on messages in a client-server environment like the one described in TS-23.140, where "SSL… is utilized to prevent some security risks presented during the exchange of data between network terminals." EX-1005, 3:61-4:4, 9:16-34, 3:44-53.

213. A POSA had multiple reasons to implement Ogawa's symmetric data encryption techniques with MMS-Rakic's system ("MMS-Rakic-Ogawa Message Encryption"), as I explain below:

214. ***First***, implementing the encryption taught in Ogawa to MMS-Rakic's system would have achieved (1) a system "having improved security" and providing "an end-user to end-user" security solution for MMS applications, as contemplated by TS-23.140, and (2) "a combination of generating a signature and encrypting the data," as Rakic contemplates. EX-1004, 19 (describing "MMS User Agent may provide additional application layer functionalities"), 24-25 (describing the MM1 interface between the MMS User Agent and the MMS Relay/Server); EX-1012, 21 ("The TLS [WP-TLS] transport layer security protocol provides for

secure data transmission between the MMS Client and the MMS Proxy-Relay in architectural configurations that employ HTTP based protocol stacks for MMS_M implementation."); EX-1007, [0075] (disclosing messages secured using "a combination of generating a signature ***and encrypting the data***" in the payload), [0078] ("Data field 822 may include content (e.g., payload)").

215. ***Second***, encrypting MMS communications using an additional layer of security beyond SSL/TLS as taught in Ogawa would have been particularly beneficial for "enterprise applications" (e.g., large-scale software systems designed to integrate and automate a company's core business processes), which a POSA understood were examples of a value-added service application that a POSA would have been motivated to ensure its MMS system could handle. EX-1027, [0002] ("an end-to-end solution is needed for large enterprises to provide a high security message solution for enterprise applications"), [0003] (describing enterprise users communicating via MMS systems), [0017] (describing " a direct communication channel between the MMS user device and the enterprise applications"), [0021]-[0022] (describing security for MMS for enterprise applications); EX-1004, 54 (describing support for transporting application data).

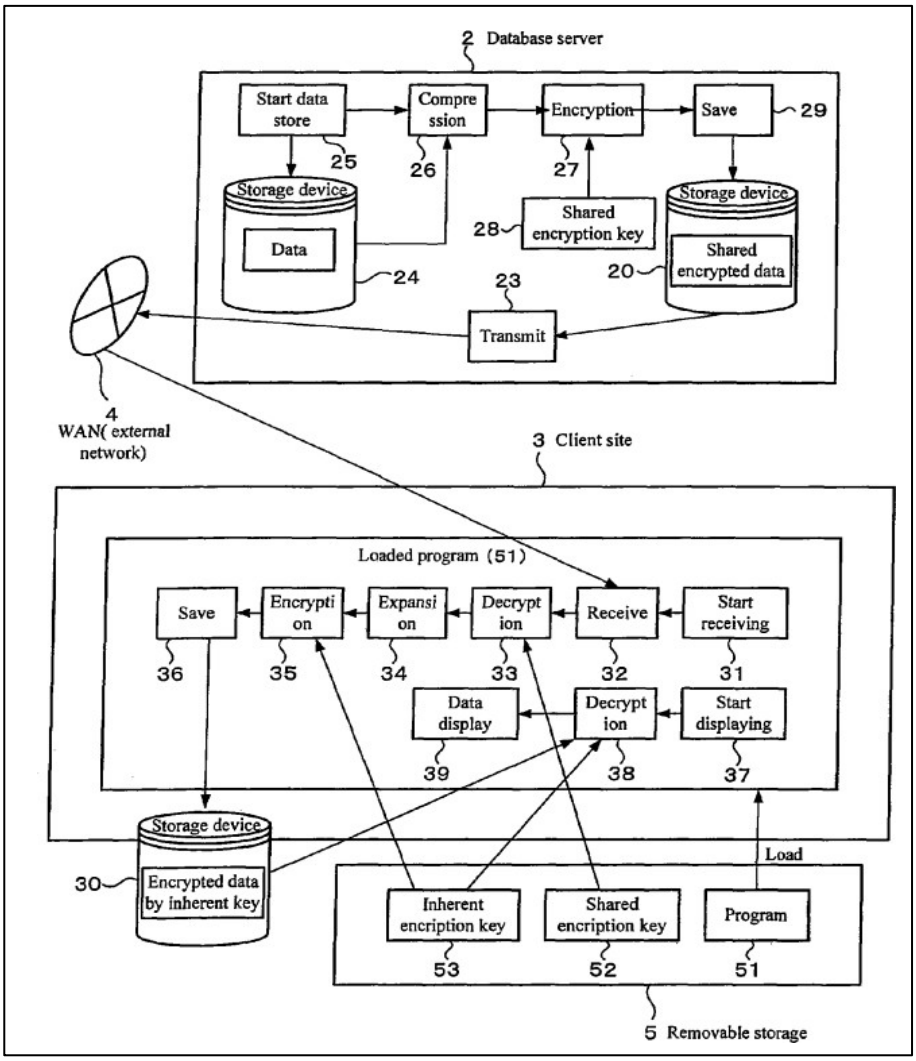
216. ***Third***, implementing Ogawa's data encryption into TS-23.140's MMS system would have been nothing more than implementing known methods/techniques (symmetric encryption using a shared key as taught in Ogawa)

to known systems/devices (the MMS Relay/Server and MMS User Agent device taught in TS-23.140) to achieve predictable results (end-user-to-end-user encrypted data, as contemplated by TS-23.140).

217. A POSA would have reasonably expected success implementing Ogawa's encryption techniques to the MMS-Rakic system given (1) the similar client-server communication architectures taught by the combined references (with connections between network elements protected by, e.g., SSL/TLS) and (2) TS-23.140's and Rakic's contemplation of end-user-to-end-user data encryption, and Ogawa provided an exemplary, predictable implementation of such encryption using a symmetric, shared encryption key. *See also* my discussion above in paragraph 212, discussing additional references that discuss use of a symmetric, shared encryption keys.

218. Specifically, in the same field of client-server communications, Ogawa explains how symmetric encryption can be implemented for securing communications in similar networked environments. Similar to TS-23.140, Ogawa uses the SSL protocol (which is a predecessor of the TLS protocol) to facilitate secure network communications between a server and a user device. EX-1005, 3:60-4:4. As illustrated in FIG. 7 of Ogawa (reproduced below), database server 2 transmits an encrypted message to client site 3 through network 4 using this secure, SSL-enabled communication link and in doing so, Ogawa seeks "to prevent some

security risks presented during the exchange of data between network terminals." EX-1005, 3:44-53; 9:16-34 (network 4 uses HTTP protocol for message transmission).



EX-1005, FIG. 7

219. Additionally, Ogawa discloses applying data encryption to messages transmitted between devices, and for such data to be encrypted, using a symmetric/shared key between the client and server, as discussed above. EX-1005, 4:53-54 (shared encryption key 14), 7:10-12 (key is transmitted to data input site

1). Ogawa provides an example of how such symmetric encryption works—i.e., by storing a shared key in each respective device's memory that would be used for both encrypting and decrypting a transmitted or received message. EX-1005, 4:48-57, 5:59-65, 6:64-7:21. This is further corroborated by Qumei. *See e.g.*, EX-1009, 3:25-27 ("an enciphering algorithm and an enciphering key may be stored in the electronic devices"), 8:1-5 ("symmetric cyphering/enciphering may use one or multiple keys for both encryption and decryption").

220. A POSA thus would have reasonably expected success implementing Ogawa's encryption teachings of using a shared encryption key to encrypt server-client communications. Such a combination would have also been predictable and straightforward to implement (and a POSA would have had a reasonable expectation of success in doing so) given (1) the similar client-server architectures taught by TS-23.140, Rakic, and Ogawa, (2) that TS-23.140 and Rakic contemplate end-to-end encryption, and (3) Ogawa provides one example and predictable implementation of such encryption using a symmetric/shared encryption key.

221. As I explain further in the following section (Section IX.B.1.b), in IPR2024-00341, the Board agreed that applying Ogawa's symmetric encryption techniques "in message transmissions like those in TS-23.140" was obvious.

b. Ogawa's Decryption Unit

222. Ogawa teaches a "decryption unit" for decrypting received encrypted data as part of its symmetric encryption system. EX-1005, 5:59-6:9 ("[R]eceived shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to the decryption unit 33 and beforehand stored…"). A POSA would have had reason to (and would have been motivated to) implement the decryption unit ***as part of MMS-Rakic's MMS User Agent*** application, because the MMS User Agent is responsible for receiving data from MMS-Rakic's Relay/Server and distributing the data to the correct applications on the user device. EX-1004, 54-56 (Section 7.1.18, Support for transporting Application Data). TS-23.140 also expressly identifies that the MMS User Agent "may provide additional application layer functionalities such as… the ***decryption***… of an MM on an end-user to end-user basis." EX-1004, 19. A POSA would have recognized that such an implementation would have, e.g., beneficially allowed MMS-Rakic's MMS User Agent to decrypt an encrypted message from MMS-Rakic's MMS Relay/Server and any information identifying the destination application to which the message should be routed—particularly in the case where the entire message is encrypted (including the identifying information specifying where to route the received message).

223. A POSA would have reasonably expected success in an implementation with Ogawa's decryption unit incorporated into MMS-Rakic's MMS User Agent application, because the prior art components would continue to perform functions they performed prior to the combination—MMS User Agents and the MMS Relay/Server would continue to exchange data using secure communication links, including Rakic's signed messages that need to be validated before being routed to identified destination applications, and Ogawa's decryption unit (as implemented as part of each MMS User Agent) would use a shared encryption key to decrypt data received from the MMS Relay/Server. In my opinion, based on my understanding of a POSA's skill as discussed in Section IV above, such a combination would have been well within a POSA's capability to implement.

224. The Board in IPR2024-00341 considered the Ogawa-based modifications of TS-23.140 that I describe in Sections IX.B.1.a and IX.B.1.b, and the Board agreed that those modifications would have been obvious, "find[ing] that the cited portions of the record support that it was known to implement symmetric encryption in message transmissions like those in TS-23.140 and that Ogawa discloses how to implement symmetric encryption," and "credit[ing] Petitioner's testimonial evidence that one of ordinary skill in the art would have implemented Ogawa's decryption… unit[] in TS-23.140 for the reasons asserted by Petitioner,

and that such implementation would have had a reasonable expectation of success, because the cited portions of the record support it." EX-1022, 42-43 (citing, e.g., EX-1004, 14, 17, 19, 24-25, 41, 54-56, 62; EX-1005, 3:60-4:4, 4:34-57, 5:59-6:9, 6:64-7:21, 8:16-19, 9:16-34, FIG. 7; EX-1009, 3:25-27, 8:1-5; EX-1012, 21; EX-1027, [0017], [0021]-[0022], [0054]-[0060]). Indeed, the Board also "determine[d]" applying Ogawa's symmetric encryption teachings (e.g., using inherent keys) to communications within MMS-Ogawa's device (EX-1038, 69-72) was likewise obvious and "fully supported by the record" (EX-1022, 50-51).

2. Claim 7: The mobile end-user device of claim 1, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes.

225. Claim 7 requires "the received secure messages" to be "encrypted," and "the device link agent" to be "configured to decrypt the received secure messages prior to delivering those messages to respective software processes."

226. As I discussed above in Section VII.D.1.h, MMS-Rakic-Ogawa's MMS User Agent (the claimed "device link agent," *see* my discussion above in Section VII.D.1.c.i) receives messages from the MMS Relay/Server over secure interface MM1. A POSA understood that "the received secure messages are encrypted," as claimed, using both MMS-Rakic-Ogawa Message Encryption (*see*

my discussion above in Section IX.B.1.a) and SSL/TLS (*see* my discussion above in Section VII.C.2).

227. In MMS-Rakic-Ogawa, such received messages are decrypted by the MMS User Agent ("device link agent," *see* my discussion above in Section VII.D.1.c.i)—which provides MMS-Rakic-Ogawa's "decryption" functionalities for encrypted MMS messages (EX-1004, 19)—using Ogawa's decryption unit, as I discussed above in Sections IX.B.1.a and IX.B.1.b.

228. As I discussed above in Sections VII.D.1.h and VII.D.1.i for [1E] and [1F], the received messages each contain an "identifier" and "application data," which, as I discussed above in Section VII.D.7, the MMS User Agent obtains for routing purposes by decrypting received encrypted messages. Thus, a POSA understood that MMS-Rakic-Ogawa's "device link agent" is "configured to decrypt the received secure messages prior to delivering those messages to respective software processes," as claimed.

C. GROUNDS 3B-3D

229. For claims 1-8, 10, and 12-14, the same reasons I described above in Section IX.B for incorporating Ogawa's teachings into MMS-Rakic apply to MMS-Rakic-Cole, MMS-Rakic-Sathish, and MMS-Rakic-Cole-Sathish (combinations that I described above in Sections VIII.A-VIII.C), because Ogawa's

teachings do not affect how and why a POSA would have combined those references.

230. Incorporating Ogawa's teachings into those three combinations render obvious claims 1-8, 10, and 12-14, for the reasons I respectively discussed above in Sections VIII.A-VIII.C—***in addition to*** claim 7 for the reasons I discussed above in Section IX.B.2.

X. GROUNDS 4A-4D

231. Claim 9 recites requirements related to a "secure execution environment" on claim 1's device. As discussed below, claim 9 is rendered obvious by incorporating Ellison's (EX-1019) teachings.

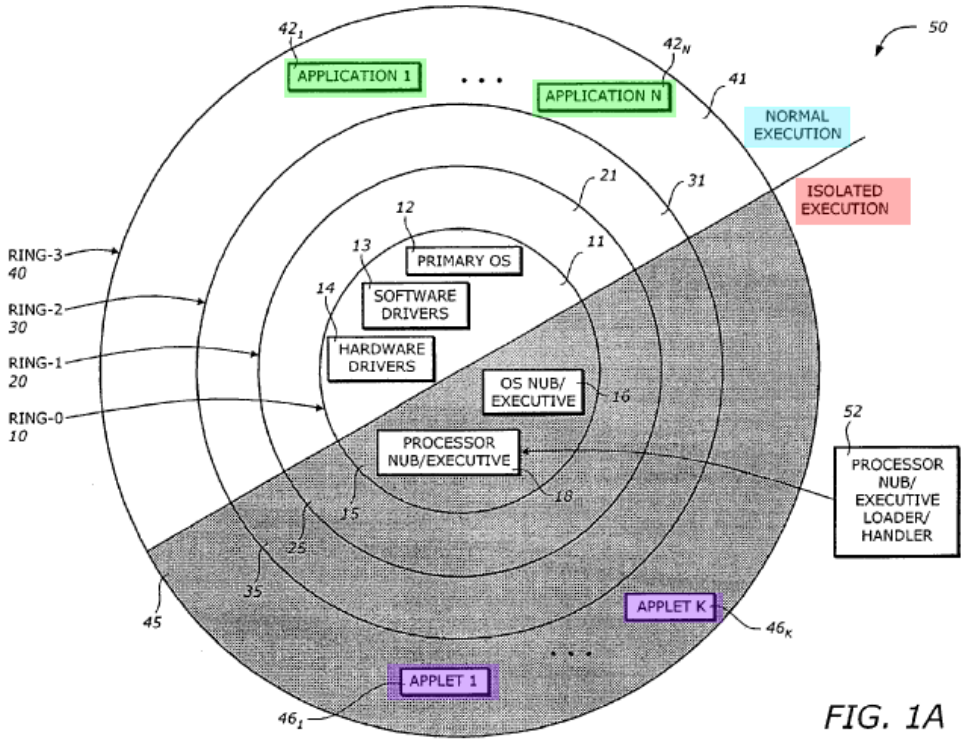
A. Ellison (EX-1019)

232. Ellison discloses techniques for "protect[ing] a subset of a software environment." EX-1019, Abstract. This includes multiple "operating system nub key[s] (OSNK)" "unique to an operating system (OS) nub." *Id*. A "usage protector" uses the OSNK to "protect usage of" a software environment's subset. *Id*.

233. Ellison FIG. 1A (annotated below) "illustrat[es] a logical operating architecture according to" Ellison's invention. EX-1019, 1:58-59. As shown below, Ellison discloses an "isolated execution mode" (red) where access "is restricted" and a "normal execution mode" (blue) that "operates in a non-secure… or normal

environment" without isolated execution mode's security features. EX-1019, 1:58-59, 3:4-6; 4:65-5:1, 6:1-26, 8:25-32, FIG. 1A-1C.

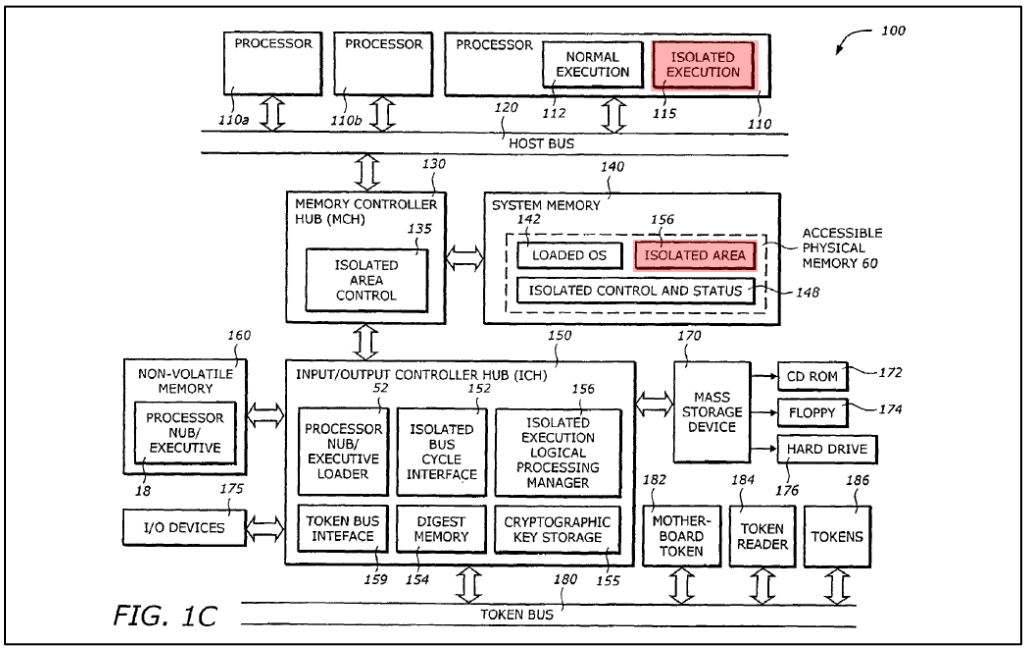
234. Ellison allows "normal" execution for applications (green) outside the device's secure platform, while "[t]he isolated mode applets [(purple)]… are tamper-resistant and monitor-resistant from all software attacks from… non-isolated space applications[.]" EX-1019, 4:1-3, 4:65-5:1.



EX-1019, Fig. 1A (annotated)

In particular, while elements ***outside*** Ellison's isolated area "***cannot*** access the isolated area," elements within the isolated area "***can*** access"—e.g., transport data to/from—the "non-isolated area." EX-1019, 4:30-37.

235. "[W]hen operating in isolated execution mode," Ellison describes processor 110 defining an "isolated area 70" in memory. EX-1019, 6:1-26, 8:25-32, FIGS. 1A-1C, 2. FIG. 1C, showing the isolated area, is reproduced below:



EX-1019, FIG. 1C (annotated)

236. FIG. 2 discloses a "secure platform" implementing Ellison's security techniques, which may wholly "operat[e] within the isolated execution environment[.]" EX-1019, 6:1-26, 8:25-32 , FIGS. 1A-1C, FIG. 2.

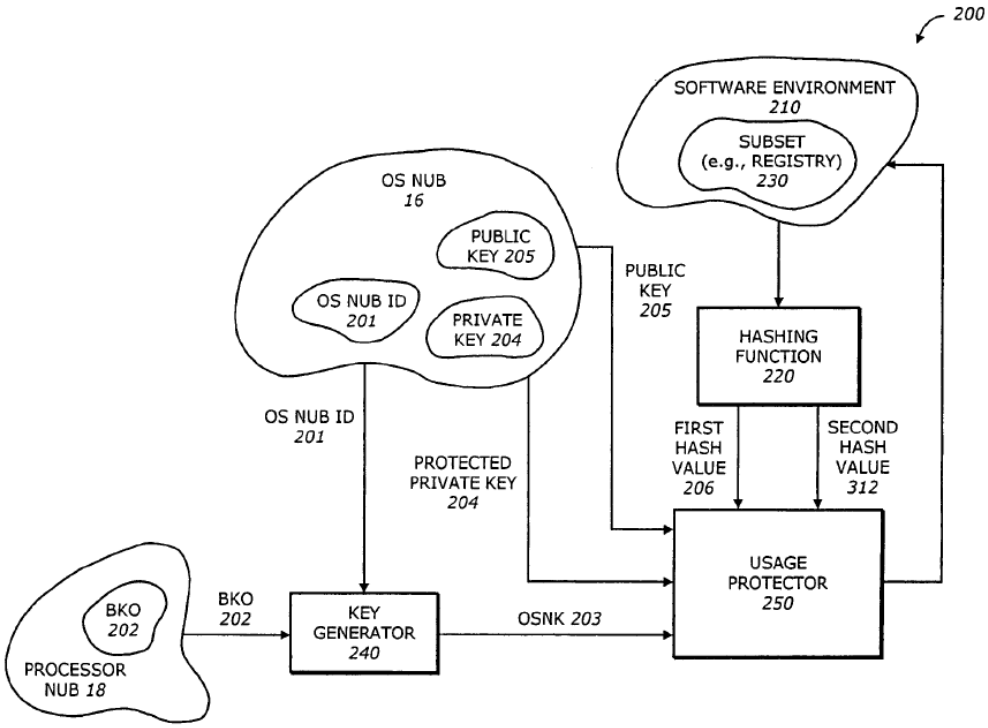


FIG. 2

237. FIG. 2's secure platform includes "key generator 240" that "generates a key operating system nub key (OSNK) 203" supplied to "usage protector 250," which uses OSNK 203 to protect subset 230's usage and OSNK 203 is supplied to "trusted agents." *Id*., 8:66-9:40, FIG. 2. One example of a trusted agent is a "usage protector 250" that "uses the OSNK 203 to protect the usage of [a] subset 230." *Id*., 9:28-40, FIG. 2. Usage protector 250 uses a hashing function with subset 230's OSNK 203 to determine if it has been altered (e.g., reads/writes to the subset 230), thereby protecting against "unauthorized reads" and detecting "intrusion, tampering or unauthorized modification." *Id*., 9:41-62, FIG. 2.

B. GROUND 4A: Implementing Ellison's Isolated Execution Environment (Claim 9)

1. MMS-Rakic-Ellison

238. A POSA had multiple reasons to implement MMS-Rakic's user devices in view of Ellison's above-described teachings of a secure platform which operates within a secure, isolated area of the user device.

239. ***First***, implementing Ellison's secure platform (EX-1019, 8:25-9:62, FIG. 2) would have desirably improved device security in the MMS-Rakic system, which transports data on behalf of applications downloaded to the device, e.g., third-party VASP applications that should not be trusted with access to sensitive device data/functions. EX-1004, 41, 54-56. The use of such secure platforms for improving device security was well-known and well-documented. *See, e.g.*, Needham (EX-1030) (describing protocol that formed basis of security protocols (e.g., Kerberos) included in many operating systems from the late 1980s and beyond); Schroeder (EX-1036) (describing "A Hardware Architecture for Implementing Protection Rings," where operating systems could allow not only for the separation of different processes depending on their security needs, but also allow for communication across such security boundaries through highly-controlled mechanisms); Saltzer (EX-1032) (describing process separation and controlled communication between processes), Li (EX-1033), 25-26 (describing the Symbian mobile operating system, which separated processes into three "Trust

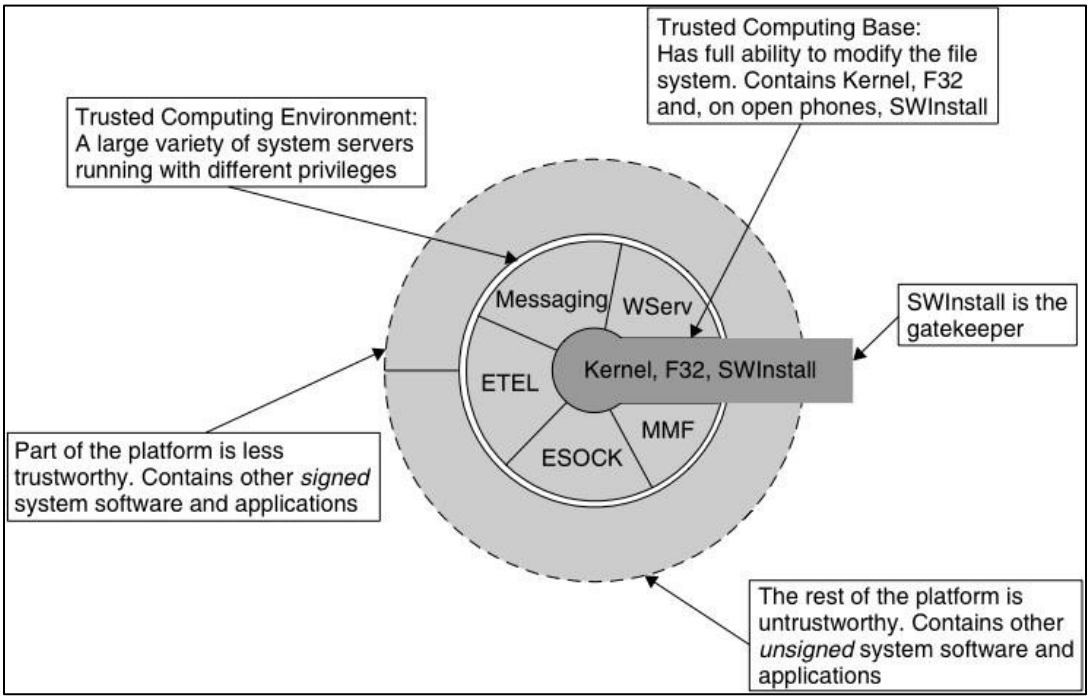
Tiers": The Trusted Computing Base (TCB), The Trusted Computing Environment (TCE), and Applications, and thereby implemented protection rings/tiers around different device components,), FIG. 1. A POSA would have been motivated to incorporate Ellison's teachings because that would have enabled intra-device message transmission with increased security and helped guard against and prevent malicious actions (malware, unauthorized access). EX-1019, 8:25-9:62, FIG. 2.

240. ***Second,*** combining TS-23.140 and Ellison's teachings merely involved combining known prior art elements (Ellison's isolated software environment in MMS-Rakic's device) according to known methods to yield predictable results.

241. A POSA would have reasonably expected success incorporating Ellison's techniques into MMS-Rakic's user devices because Ellison expressly describes that its techniques can be implemented in "computer system[s]" (like MMS-Rakic's user devices) with "processor[s]." EX-1019, 5:11-16.

242. Moreover, it was well-known for computing systems to include the messaging services and clients/agents responsible for providing those services, ***within*** a trusted/secure computing environment, and for applications (e.g., downloaded third-party destination applications to which messages are directed) to be tiered/organized outside this environment. This is confirmed, for example, by Li (EX-1033). Li establishes that in the early 2000s, the Symbian mobile operating

system separated processes into three "Trust Tiers": The Trusted Computing Base (TCB), The Trusted Computing Environment (TCE), and Applications, as illustrated below:



EX-1033, 25-26, FIG. 1. As shown above, the first two layers/tiers shown were primarily dedicated to components of the Operating System with relatively higher operating privileged, followed by the Applications tier with applications having relatively lower privileges. *Id.* The first two tiers included the Trusted Computing Base and the Trusted Computing Environment. *Id.* As shown, the Trusted Computing Environment includes, among other services, a Messaging service. *Id.* The Application Tier could be further subdivided into Signed and Unsigned applications. *Id.* Signed applications could interact with the TCE and have this

layer execute higher privileged requests, whereas Unsigned applications could not access that same functionality. *Id.*

243. Given (1) the fact that TS-23.140 expressly contemplates a user device with an MMS User Agent that communicates with downloaded applications on the user device (e.g., a downloaded application trying to upload messages transporting application data to the MMS Relay/Server via the MMS User Agent), (2) the well-known need to protect computing environments (including components providing essential services such as messaging) from other applications/components of the environment, and (3) Ellison's own disclosures confirming the same, a POSA would have been motivated to implement Ellison's teaching of a secure execution environment that enables such improved security within the MMS environment, such that the MMS User Agent is organized as part of the trusted computing environment (i.e., the secure execution environment) and enables communications with applications residing outside this trusted/secure environment. As noted above, Ellison expressly discloses elements ***outside*** of Ellison's isolated area not being able to "access the isolated area," while elements within the isolated area "***can*** access"—e.g., transport data to/from—the "non-isolated area." EX-1019, 4:30-37.

244. In such an implementation ("MMS-Rakic-Ellison"), Ellison's secure platform is incorporated into TS-23.140's user devices to secure the MMS User

Agent, with a usage protector protecting messaging operations of the MMS User Agent. EX-1019, 8:25-32, 8:66-9:62, FIG. 2. The MMS User Agent runs within subset 230 of software environment 210 in "isolated execution mode," while at least one device application runs in "normal execution mode." EX-1019, 3:4-6. As noted (e.g., paragraphs 235-237), Ellison allows for "normal" execution for applications outside of the secure execution environment on that device. EX-1019, 4:65-67, 5:1, 6:1-26, FIGS. 1A, 1C. Ellison's usage protector provides secure access to applications residing outside the secure execution environment. EX-1019, 8:25-32, 8:66-9:62, FIG. 2.

2. Claim 9: The mobile end-user device of claim 1, wherein the device link agent executes in a secure execution environment, and at least one of the software components executes outside of the secure execution environment.

245. Claim 9 requires that the "device link agent executes in a secure execution environment," while "at least one of the software components executes outside of the secure execution environment."

246. MMS-Rakic-Ellison, which incorporates Ellison's secure platform teachings into MMS-Ogawa's device, meets claim 9. A POSA understood that Ellison's secure, isolated area is a "***secure execution environment***," as claimed. A POSA further understood that MMS-Rakic-Ellison's MMS User Agent executes in the "secure execution environment," while at least one un-trusted third-party device application (one of the claimed "plurality of software components")

"executes outside of the secure execution environment" (*see* my discussion above in Section X.B). As discussed, the MMS User Agent, which handles potentially sensitive user data in transit over the network, executes in the isolated environment of MMS-Rakic-Ellison. By contrast, destination applications on the user device—which do not directly transmit such data outside of the device or establish the connection between the User Agent and the Relay/Server—execute outside the isolated environment because they require lower security due to handling lower sensitivity information (e.g., chess game handling chess moves). EX-1004, 55.

247. As required by Element [1F], MMS-Rakic-Ellison's "device link agent" still has authorized communications with the "software components[] execut[ing] outside of the secure execution environment" over the "inter-process software communication bus" as claimed.

C. GROUNDS 4B-4D

248. For claims 1-8, 10, and 12-14, the same reasons I described above in Section X.B.1 for incorporating Ellison's teachings into MMS-Rakic also apply to MMS-Rakic-Cole, MMS-Rakic-Sathish, and MMS-Rakic-Cole-Sathish (combinations, which I described above in Sections VIII.A-VIII.C), because a POSA understood that Ellison's teachings do not affect how and why a POSA would have combined those references as discussed for those claims.

249. Incorporating Ellison's teachings into those three combinations render obvious claims 1-8, 10, and 12-14 for the reasons I respectively discussed above in Sections VIII.A-VIII.C—***in addition*** to claim 9 for the reasons I discussed above in Section X.B.2.

XI. GROUNDS 5A-5D

250. Claim 11 requires that claim 10's "device link agent" be "configured to buffer" claim 10's "upload messages for transmission to the network message server at a time selected by a heartbeat mechanism." As I discuss below, claim 11 is rendered obvious by incorporating Shen's (EX-1027) teachings.

A. Shen (EX-1027)

251. Shen discloses a "[MMS] system" in which a "[MMS] user device communicates with [a MMS] gateway via [a] wireless LAN… to send and receive multimedia messages." EX-1027, Abstract, [0001] (Shen's "invention relates to multimedia message service (MMS), particularly a multimedia messaging service system, a gateway and a user device" and "a method for receiving/sending multimedia message."). Shen's user device comprises "a heartbeat sender" which "sends heartbeat signals periodically" to the MMS gateway, which records the transmitted information in the presence manager, to determine whether the device "is located in the coverage of the wireless LAN." EX-1027, [0018], [0033]-[0034], Fig. 5 (annotated).

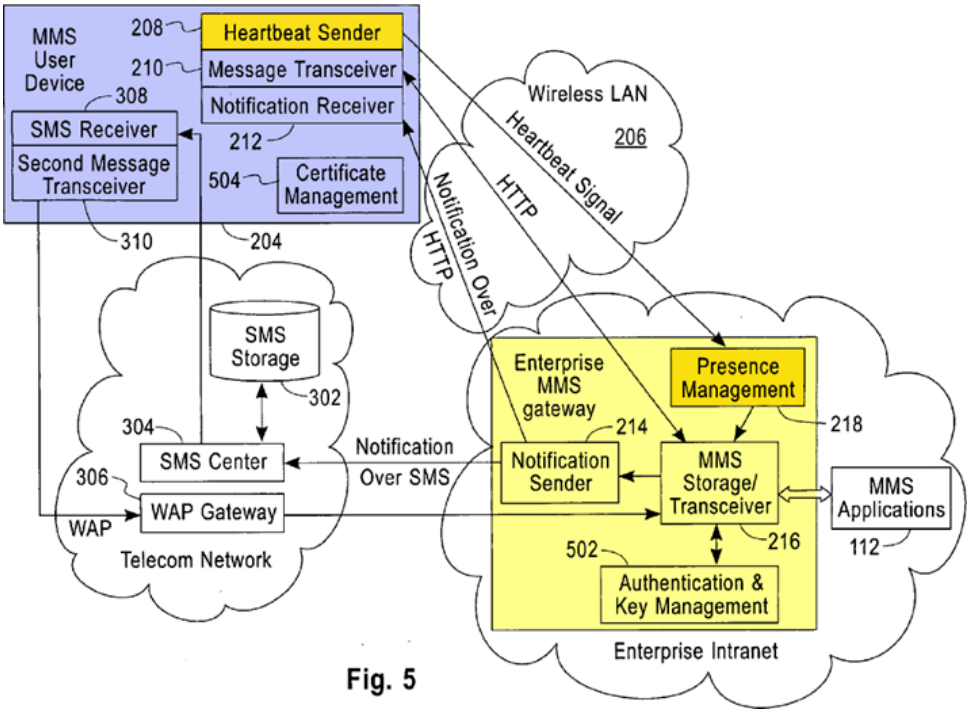


Fig. 5

252. If the gateway receives the heartbeat signal, the client is available, and the gateway informs the user of pending messages. EX-1027, [0034] (When "the gateway periodically receives the heartbeat signals, it means the corresponding user is located in the coverage of the wireless LAN, and the gateway may send a notification to the user when there is a message to be sent to that user."). Otherwise, the user is unavailable (e.g., offline or outside of the wireless LAN's coverage), "and the gateway does not send any notification to the user even if there is a MMS message to be sent to that user." *Id*.

B. GROUND 5A: Implementing Shen's Heartbeat Teachings

1. MMS-Rakic-Shen

253. TS-23.140 expressly identifies the MMS User Agent as being responsible for "all aspects of storing MMs on the terminal[.]" EX-1004, 19. TS-

23.140 also discloses storing data that it intends to submit to an MMS Relay/Server that is unreachable "***in the UE*** until the recipient MMS Relay/Server becomes reachable." EX-1004, 35-36 (discussing read-reply reports). *See also* EX-1004, 29 ("the recipient MMS Relay/Server" "shall store messages in the network until the recipient MMS User Agent becomes reachable (e.g. user moves back into coverage, switches MMS User Agent on)….").

254. However, TS-23.140 does not disclose details regarding (1) how an MMS User Agent determines when an unreachable MMS Relay/Server "***becomes reachable***," or (2) how an MMS User Agent handles messages it receives from device applications (for relaying to a MMS VAS Application) while waiting for ***an unavailable MMS Relay/Server*** to ***"become[] reachable."*** EX-1004, 19.

255. One solution for handling such scenarios (in which a message recipient is unavailable), which was well-known to a POSA, was by using heartbeat signals to periodically (rather than continuously) check for availability and buffering pending messages until the recipient became available. EX-1027, [0018], [0033], [0034] ("MMS user device sends heartbeat signals periodically to the enterprise MMS gateway…. If the gateway periodically receives the heartbeat signals, it means the corresponding user is located in the coverage of the wireless LAN, and the gateway may send a notification to the user when there is a message to be sent to that user"); EX-1040, [0011] (disclosing an IP gateway that, upon

receiving a heartbeat message from a client device, "determine[s] whether there are any pending messages or other data for the device" "and transmits the message or data to the device"); *see also* EX-1061, [0088] (disclosing "Batch Processing of Message Transactions" in a wireless messaging system at periodic intervals), [0042] (disclosing "output queue… for storing outgoing messages"), [0094] ("message transactions occurring over ***periodic intervals*** (e.g., every 10 minutes) may be combined and transmitted at the end of each interval"); EX-1062, 1:54-2:3 (disclosing data synchronization operations with server that are triggered by a mobile device and "performed periodically" in order to avoid "wast[ing] limited wireless bandwidth and plac[ing] an undue drain on the mobile device's battery"), 13:33-36, 16:37-53, FIGS. 11-12A. Shen discloses details regarding how to implement such heartbeat signals in an MMS system like TS-23.140's. EX-1027, [0018], [0033]-[0034]. A POSA had multiple reasons to implement MMS-Rakic in view of Shen's heartbeat signal teachings.

256. ***First***, it was well-known that heartbeat messages were small, typically encompassing far less data than MMs. EX-1043, [0062] (providing an example "64-byte link heartbeat (HB) message"), as opposed to kilobytes or even megabytes for MMs (to transmit multimedia such as images and video)). To conserve network bandwidth, a POSA would have been motivated to implement UE/devices to send a small amount of data to confirm that a connection to a

previously unreachable message recipient—e.g., an MMS Relay/Server—was alive again before attempting transmission of larger MMs that have, e.g., been buffered on the device and await uploading to the MMS Relay/Server. *E.g.*, EX-1044, cl. 14 (describing "receiving data from the mobile device in the network, receipt of data from the mobile device occurring only after receipt of the connection confirm message in the mobile device."); EX-1061, [0091] (discussing use of batch-processing for "conserv[ing] bandwidth"), [0094] (discussing "periodic" message transactions where messages are "combined" and "transmitted together"), EX-1062, 1:54-2:3 (discussing "periodic[]" data synchronization to avoid "wast[ing] limited wireless bandwidth").

257. ***Second,*** a POSA understood that combining TS-23.140 and Shen's teachings involved combining known prior art elements (Shen's heartbeat mechanism in MMS-Rakic's device) according to known methods to yield predictable results.

258. A POSA would have reasonably expected success incorporating Shen's techniques into MMS-Rakic's user devices because Shen describes its techniques implemented in a "MMS system." EX-1027, [0018], [0033]-[0034]. A POSA understood that MMS-Rakic and Shen already provided the necessary software elements to carry out the modification—including a heartbeat mechanism for sending heartbeat messages—and that incorporating Shen's techniques into

MMS-Rakic's user devices would simply require adjusting timers to trigger message delivery after the heartbeat confirmed the reachability of the MMS Relay/Server.

259. In such an implementation, MMS-Rakic's user device would be implemented to store ("buffer") messages until they are able to be sent to an unreachable MMS Relay/Server (EX-1004, 19, 35-36) and Shen's "heartbeat sender" would be used "to determine whether [the MMS Relay/Server] is available." EX-1027, [0033]-[0034].

2. Claim 11

260. Claim 11 recites that the "device link agent" is "configured to buffer one or more of" claim 10's "upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."

261. As I discussed above in Section VII.D.9, "network message server" has no antecedent basis and at minimum encompasses claim 1's "message link server." As I discussed above in Sections XI.B and VII.D.9, MMS-Rakic-Shen's MMS User Agent stores upload messages received from device applications until it is able to transmit the messages to the MMS Relay/Server—which occurs once the heartbeat mechanism confirms that MMS Relay/Server is available.

C. GROUNDS 5B-5D

262. For claims 1-8, 10, and 12-14, the same reasons I described above in Section XI.B.1 for incorporating Shen's teachings into MMS-Rakic also apply to MMS-Rakic-Cole, MMS-Rakic-Sathish, and MMS-Rakic-Cole-Sathish (combinations, which I described above in Sections VIII.A-VIII.C), because a POSA understood that Shen's teachings do not affect how and why a POSA would have combined those references.

263. Incorporating Shen's teachings into those three combinations render obvious claims 1-8, 10, and 12-14 for the reasons I respectively discussed above in Sections VIII.A-VIII.C—***in addition*** to claim 11 for the reasons I discussed above in Section XI.B.2.

XII. CLAIM LISTING APPENDIX

Claim 1
[1PRE] A mobile end-user device comprising:
[1A] a wireless modem configurable to exchange data via a connection to a wireless network;
[1B1] an inter-process software communication bus providing secure communication between an executing device link agent and respective executing processes for a plurality of software components,
[1B2] wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and
[1C] the device link agent, configured to
[1D1] maintain a secure message link through the wireless network and an Internet network to a message link server,
[1D2] the message link server operating a message service that receives messages over a network from a plurality of network functions,
[1E] receive secure messages from the message link server over the secure message link, the received messages identified for delivery to multiple ones of the software components, and including message content received by the message link server from multiple ones of the network functions, and
[1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component.
Claim 2
The mobile end-user device of claim 1, wherein the access authorization information provided by the secure server for a given one of the software components comprises a signature.

Claim 3
The mobile end-user device of claim 1, wherein the software components include a first device component that receives message content in a first format, and a second device component that receives message content in a second format different than the first format.
Claim 4
The mobile end-user device of claim 3, further comprising a user interface, wherein the first device component is a user service interface agent, and the first format comprises a notification message, the user service interface agent configured to display the notification message on the user interface.
Claim 5
The mobile end-user device of claim 4, the user service interface agent further configured to obtain a user input as a response to the display of the notification message, and deliver the user input to an agent on the device.
Claim 6
The mobile end-user device of claim 3, wherein the first device component is a policy control agent, and the first format contains service settings and/or configuration information.
Claim 7
The mobile end-user device of claim 1, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes.
Claim 8
The mobile end-user device of claim 7, wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.
Claim 9
The mobile end-user device of claim 1, wherein the device link agent executes in a secure execution environment, and at least one of the software components executes outside of the secure execution environment.

Claim 10
The mobile end-user device of claim 1, wherein the device link agent is further configured to receive, from one or more of the authorized software components, upload messages, each of the upload messages identifying a corresponding one of the network functions to which the device respective software component has requested delivery, the device link agent transmitting the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements.
Claim 11
The mobile end-user device of claim 10, the device link agent further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism.
Claim 12
The mobile end-user device of claim 1, wherein at least one of the secure messages received from the network message server comprises multiple identifier/data pairs.
Claim 13
The mobile end-user device of claim 2, wherein the given one of the software components is identified by a secure unique identifier.
Claim 14
[14PRE]A method of operating a mobile end-user device having a wireless modem to connect to a wireless network, the method comprising:
[14A] receiving access authorization information from a secure server;
[14B] operating an inter-process software communication bus to provide secure communication between an executing device link agent and respective executing processes for a plurality of software components, the secure communication comprising allowing access to the bus only for software components identified by the access authorization information;
[14C] maintaining a secure message link from the device link agent through the wireless network and an Internet network to a message link server, the message link server operating a message service that receives messages over a network from a plurality of network functions;

[14D] receiving secure messages at the device link agent from the message link server over the secure message link, the received messages identified for delivery to multiple ones of the software components, and including message content received by the message link server from multiple ones of the network functions; and
[14E] for software components identified by the access authorization information, routing messages identified for delivery to a given one of those software components via the inter-process software communication bus from the device link agent to a software process corresponding to the given software component.

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

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

Dated: 26 March 2026

Dr. Patrick G. Traynor

APPENDIX A

Patrick Gerard Traynor

Professor
Interim Department Chair 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) . . . 23
  - E.3. Conference Presentations without Proceedings . . . 23
- F. Other . . . 23
  - F.1. Submitted Journal Papers . . . 23
  - F.2. Refereed Research Reports . . . 23
  - F.3. Software . . . 23
  - F.4. Published Papers (Non-Refereed) . . . 23
  - F.5. Books in Preparation . . . 24
  - F.6. Workshops and External Courses . . . 24
- G. Research Proposals and Grants (Principal Investigator) . . . 24
- H. Research Proposals and Grants (Contributor) . . . 27
- I. Research Honors and Awards . . . 29

III. SERVICE **30**
- A. Professional Activities . . . 30
  - A.1. Memberships and Activities in Professional Societies . . . 30
  - A.2. Conference Committee Activities . . . 30
- B. On-Campus Committees . . . 31
  - B.1. University of Florida . . . 31
  - B.2. Georgia Tech . . . 32
- C. Special Assignments . . . 32
- D. Ph.D. Examining Committees . . . 32
- E. External Member of M.S. Examining Committee . . . 36
- F. Consulting and Advisory Appointments . . . 36
- G. Civic Activities . . . 36

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION **37**
- A. Honors and Awards . . . 37
- B. Invited Conference Session Chairmanships . . . 37
- C. Professional Registration . . . 37
- D. Patents . . . 37
- E. Editorial and Reviewer Work for Technical Journals and Publishers . . . 38
- F. Expert Witness Services . . . 40

V. OTHER CONTRIBUTIONS **42**
- A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia) . . . 42

B. Special Activities 46

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
Interim Department Chair	University of Florida	*July 2025–Present*
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, voice-driven systems, 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 the use of AI in generating non-consensual imagery. Now Research Scientist at ActiveFence.

Seth Layton University of Florida
Fall 2020–Summer 2025
Detecting deepfakes in audio samples. Now Research Scientist at PinDrop.

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

Tyler Tucker University of Florida
Fall 2021–Summer 2025
Evaluating the security of Bluetooth/cellular radios. Now: Associate at the Analysis Group.

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

Kevin Warren University of Florida
Fall 2019–Summer 2025
Detecting deepfake audio through linguistic information. Now: Associate at the Analysis Group.

2. Ph.D. Students Supervised

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

Jordan Greene University of Florida
Fall 2025–Present
Defending voice-driven systems and cellular network security.

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.

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.

Aviva Smith University of Florida
Fall 2025–Spring 2026
Detecting attacks on voice-driven systems and deepfakes.

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. Kevin Butler, Kurt Hugenberg, Eakta Jain, Apu Kapadia Tadayoshi Kohno, Elissa Redmiles, Franziska Roesner, Mattea Sim, Patrick Traynor, and Hanna Barakat. Extending the Heilmeier Catechism to Evaluate Security and Privacy Systems: Who is Left Out? *IEEE Security and Privacy*, May/June 2025.

2. 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%).

3. 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.

4. 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.

5. 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.

6. 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.

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

8. 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.

9. 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.

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

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

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

23. 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.

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

25. 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.

26. 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.

27. 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.

28. 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.

29. 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. Seaver Thorn, Nathaniel Bennett, Kevin Butler, Patrick Traynor, and William Enck. ASN1spect: Uncovering ASN.1 Compiler-Generated Vulnerabilities in Critical Infrastructure. In *ACM Secure Development (SecDev) Conference*, 2026.

2. Eric Pauley and Yohan Beugin and Paul Barford and Patrick Traynor and Patrick McDaniel. Honey Configs: Measuring the Disclosure and Exploitation of Cloud IP Address Reuse. In *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2026.

3. Nathaniel Bennett, Tyler Tucker, Carson Stillman, William Enck, Patrick Traynor, and Kevin Butler. Fizzle: A Framework for Deterministic and Reproducible Network Fuzzing. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2026.

4. Seth Layton, Bernardo Medeiros, Kevin Butler, and Patrick Traynor. AI Wrote My Paper and All I Got Was This False Negative: Measuring the Efficacy of Commercial AI Text Detectors. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2026.

5. Carson Stillman, Jennifer Sheldon, Ian Garrett, Patrick Traynor, Ryan Gerdes, Sara Rampazzi, and Kevin Butler. EM-Flow: Advanced Electromagnetic Control Flow Verification for Embedded Systems. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2025.

6. Daniel Olszewski, Tyler Tucker, Kevin Butler, and Patrick Traynor. SoK: Towards a Unified Approach to Applied Replicability for Computer Security. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.

7. Daniel Olszewski, Allison Lu, Anna Crowder, Nathaniel Bennett, Seth Layton, Sri Hrushikesh Varma Bhupathiraju, Tyler Tucker, Siddhant Kalgutkar, Hunter Ver Helst, Carson Stillman, Kevin Butler, Sara Rampazzi, and Patrick Traynor. Reproducibility in Applied Security Conferences: An 11-Year Review on Artifacts and Evaluation Committees. In *Proceedings of ACM Conference on Reproducibility and Replicability (REP)*, 2025.

8. 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.

9. 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%).

10. Anna Crowder, Allison Lu, Kevin Childs, Carson Stillman, Patrick Traynor, and Kevin Butler. Data to Infinity and Beyond: Examining Data Sharing and Reuse Practices in the Computer Security Community. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2025.

11. 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%).

12. 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%).

13. 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%).

14. 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%).

15. 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%).

16. 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).

17. 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%).

18. 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.

19. 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%).

20. 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%).

21. 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%).

22. 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%).

23. 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%).

24. 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.

25. 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%).

26. 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%).

27. 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%).

28. 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%).

29. 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.

30. 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.

31. 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%).

32. 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%).

33. 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.

34. 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%).

35. 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).

36. 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).

37. 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%).

38. 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%).

39. 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%).

40. 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%).

41. 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%).

42. 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%.

43. 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%.

44. 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%.

45. 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.

46. 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.

47. 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%).

48. 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%).

49. 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%).

50. 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%).

51. 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%).

52. 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%).

53. 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%).

54. 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%).

55. 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%).

56. 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%).

57. 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%).

58. 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%).

59. 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%).

60. 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%).

61. 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%).

62. 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%).

63. 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%).

64. 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%).

65. 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%).

66. 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%).

67. 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%).

68. 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).

69. 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%).

70. 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).

71. 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).

72. 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%).

73. 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%).

74. 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%).

75. 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%).

76. 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%).

77. 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%).

78. 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%).

79. 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%).

80. 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%).

81. 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%).

82. 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%).

83. 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%).

84. 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%).

85. 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%).

86. 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%).

87. 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%).

88. 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%).

89. 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%).

90. 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%).

91. 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).

92. 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%).

93. 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%).

94. 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%).

95. 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%).

96. 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%).

97. 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%).

98. 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%).

99. 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%).

100. 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. **Reconstructing Human Physiological Features from Audio Samples**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *$700,000 over 3 years*
Awarded: August 2021

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

5. **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

6. **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

7. **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

8. **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

9. **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

10. **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

11. **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

12. **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

13. **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

14. **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

15. **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

16. **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

17. **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

18. **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

19. **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

20. **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

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **RADIOBEAR**
   Sponsor: Nightwing Intelligence / US Air Force
   Investigator(s): Kevin Butler (PI), Patrick Traynor
   Amount: *$249,327 for 1 year*
   Awarded September 2025

2. **Artus Protocol STTR Phase II - Extension**
   Sponsor: Office of Naval Research
   Investigator(s): Kevin Butler (PI), Patrick Traynor
   Amount: *$300,000 over 1 year*
   Awarded: August 2024

3. **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

4. **Mobile Interface Security Analysis**
   Sponsor: Office of Naval Research
   Investigator(s): Kevin Butler (PI), Patrick Traynor
   Amount: *$700,000 over 3 years*
   January 2020

5. **AFOSR University Center of Excellence in Assured Autonomy in Contested Environments (AACOE)**
   Sponsor: Air Force Office of Scientific Research and Air Force Research Labs
   Investigator(s): Warren Dixon (PI), Patrick Traynor
   Amount: *$5,999,515 for 5 years*
   March 2019

6. **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

7. **Smartphones and Mobile Money: Analysis and Recommendations for Security**
   Sponsor: GSMA Mobile For Development Foundation
   Investigator(s): Kevin Butler (PI), Patrick Traynor
   Amount: *$28,500*
   December 2017

8. **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*
   December 2016

9. **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*
   October 2016

10. **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*
    September 2015

11. **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

12. **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

13. **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

14. **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

15. **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

16. **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. Social Impact Award, New York University CSAW Applied Research Competition, 2025.
2. Distinguished Paper (Runner Up), USENIX Security Symposium, 2025.
3. Best Paper Award, ACM Conference on Reproducibility and Replicability (REP), 2025.
4. Distinguished Paper, ACM Conference on Computer and Communications Security (CCS), 2024.
5. Best Paper Award, ACM Conference on Data and Application security and Privacy (CODASPY), 2024.
6. Distinguished Paper, USENIX Security Symposium, 2018.
7. Fellow, Center for Financial Inclusion at Accion, 2017.
8. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.
9. Best Paper, The ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec); Budapest, Hungary, 2013.
10. Best Student Paper, The Information Security Conference (ISC); Passau, Germany, 2012
11. Lockheed Inspirational Young Faculty Award, 2012
12. Best Demo, "Is Browsing the Internet on Your Mobile Phone Secure?" Chaitrali Amrutkar (Ph.D Advisee), CoC Research Day, 2011
13. 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
14. National Science Foundation CAREER Award, 2010
15. Pennsylvania State University Alumni Association Dissertation Award, 2007
16. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
17. 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. *Natalie Delgado, et al. v. Meta Platforms Inc., Case No.: 23-cv-04181 (N.D. Cal.):* Expert witness for the Defense (via Gibson, Dunn & Crutcher, LLP). *October 2025 - Present*.
2. *Google LLC v Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Wolf, Greenfield & Sacks, P.C.). *August 2025 - Present*.
3. *Amazon v Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Perkins Coie, LLP). *August 2025 - Present*.
4. *HBCU Messaging US LP v. Apple, Inc. et al., Civil No. 1:24-cv-1199,:* Expert witness for the Defense (via Fish & Richardson, LLP). *June 2025 - Present*.
5. *PACid v. Citibank, N.A., 1:24-cv-00272-DAE (W.D. Tex.):* Expert witness for the Defense (via Troutman Pepper Locke LLP). *April 2025 - November 2025*.
6. *Facebook Inc. Derivative Litigation., Consolidated C.A. No. 2018-0307-JTL (Del. Ch.):* Expert witness for the Defense (via Wachtell, Lipton, Rosen & Katz, LLP) *January 2025 - July 2025*.
7. *Averon US, Inc. vs AT&T Inc., Case No. 1:22-cv-01341-TMH:* Expert witness for the Defense (via O'Melveny & Myers, LLP). *November 2024 - September 2025*.
8. *RightQuestion, LLC v. AT&T Inc. et al.,., Case No. 2-24-cv-00094 -JRG:* Expert witness for the Defense (via Duane Morris, LLP). *September 2024 - November 2025*.
9. *ByteDance Ltd. vs CellSpin Soft, Inc.:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *February 2024 - October 2024*.
10. *Bank of America, N.A., vs PACid:* Expert witness for the Plaintiff for Inter Partes Review (via McNish PLLC). *December 2023 - March 2024*.
11. *Microsoft vs Proxense, LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *November 2023 - July 2025*.
12. *Samsung vs Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *August 2023 - October 2025*.

13. *Advanced Coding Technologies LLC v. ByteDance PTE. Ltd., and TikTok PTE. Ltd.:* Expert witness for the Defense for Non-Infringement (via Fish & Richardson, LLP). *July 2023 - September 2023.*

14. *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). *January 2023 - June 2024.*

15. *Rubin vs KAHOOT! ASA and KAHOOT EDU:* Expert witness for the Defendant for Inter Partes Review (via Vasquez Benisek & Lindgren, LLP). *December 2022 - June 2024.*

16. *Telefonaktiebolaget LM Ericsson vs Apple, Inc:* Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). *February 2022 - December 2022.*

17. *Wepay Global Payments, LLC v. Bank of America N. A.,:* Expert Witness for the Defendant (via WilmerHale LLP) *September 2022 - November 2022.*

18. *Apple vs. R.N Nehushtan Trust Ltd.:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *August 2022 - June 2023.*

19. *Apple/Microsoft vs. Zipit Wireless:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *May 2021 - November 2022.*

20. *Blackberry Inc v MobileIron, Inc:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *January 2021 - March 2021.*

21. *Apple Inc v Seven Networks, LLC:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *August 2019 - November 2020.*

22. *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). *October 2017 - December 2018.*

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

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

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

26. *Maxim Integrated Products v Bank of the West:* Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). *January 2014 - August 2014.*

27. *Maxim Integrated Products v Comerica Inc, et al:* Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). *June 2014 - August 2014.*

28. *William Grecia v. Apple Inc. et al:* Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). *July 2014 - August 2014.*

29. *Intertrust Technologies Corp. v. Apple Inc.:* Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). *October 2013 - February 2014.*

30. *Maxim Integrated Products v KeyCorp Bank:* Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) *April 2013 - June 2013.*

31. *Intellectual Ventures LLC vs. Check Point; et al.:* Expert Consultant for the Plantiff for Infringement (via Susman Godfrey LLP), *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.